European Commission

JRC SCIENCE FOR POLICY REPORT

Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)

Administrative Arrangement

JRC 33516-2014

Laurent Beslay
Javier Galbally

2015

Joint Research Centre

EUR 27473 EN

JRC Science Hub
https://ec.europa.eu/jrc

JRC97779

EUR 27473 EN

PDF ISBN 978-92-79-51929-1 ISSN 1831-9424 doi:10.2788/50621 LB-NA-27473-EN-N

How to cite: L.Beslay, J.Galbally; Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II); EUR 27473 EN; 10.2788/50621

Abstract
Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)
This report presents the results of a JRC study on the readiness and availability of Automatic Fingerprint Identification System (AFIS) technologies for their introduction in the second generation Schengen Information System (SIS-II), The study summarises a review of the scientific literature, visits to authorities managing AFIS in nine Member States and in the United States of America and consultations with eu-LISA and with AFIS vendors. An external scientific board of international experts reviewed the results and conclusions of the study. The report concludes that AFIS technology has reached a satisfactory level of readiness and availability and proposes a series of recommendations in order to accomplish a successful implementation of a SIS-II AFIS.

Executive summary

This report details the results of a JRC study on the readiness and availability of Automatic Fingerprint Identification System (AFIS) technologies for their introduction in the second generation Schengen Information System (SIS-II). The study was carried out for DG HOME via an Administrative Arrangement.

Policy context

Created as a compensatory measure for the abolition of internal border checks within the Schengen area, the Schengen Information System (SIS) was established with two intentions: to contribute to law enforcement cooperation between the Member States and to support external border control. The SIS was the first so-called large-scale IT system launched by the EU Member States in 1995. It was followed by EURODAC (asylum seekers' database) in 2003 and the Visa Information System (VIS) in 2011. The second generation of the system, SIS-II, entered into operation on 9 April 2013.

SIS-II enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. In the case of alerts related to persons, SIS-II offers the possibility to process biometric data. However the possibility to *identify* a person on the basis of his/her fingerprints – a functionality which would require the implementation of an Automatic Fingerprint Identification System (AFIS) – is conditional on the preparation of "*a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted*" (see Articles 22(c) of SIS-II Decision[1] and Regulation[2]).

The objectives of the study are to address the requirement stated in Article 22(c) and to provide information on whether fingerprint identification technology is mature enough for its integration into SIS-II.

The report presents the main findings of the study together with a series of recommendations for successful implementation of AFIS functionality. The complete technical specification of an AFIS for SIS-II would still require further study.

The JRC conducted an in-depth analysis of AFIS technology including: a review of the scientific literature, visits to authorities managing AFIS in nine Member States and in the United States of America and consultations with eu-LISA[3] and with AFIS vendors. An external scientific board of renowned international experts reviewed the results and conclusions of the study.

The report has two main parts:

- Part I presents the current status of AFIS technology, introducing key concepts such as accuracy and biometric quality and concluding with the main challenges faced in the design and deployment of AFIS functionality in a large-scale IT-system.
- Part II analyses the current implementation of SIS-II and puts forward recommendations to address the challenges identified in Part I in order to successfully implement AFIS functionality in SIS-II in the most effective way possible.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0004:EN:PDF

[3] eu-LISA is the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

Key conclusions

For more than 35 years AFIS functionality has been intrinsically linked with databases supporting law enforcement and border management activities. According to its general purpose, SIS-II constitutes one of those databases and therefore SIS-II alerts related to persons will not deliver their full capacity and usefulness without the support of an Automatic Fingerprint Identification System.
AFIS technology has reached sufficient levels of readiness and availability for its integration into SIS-II, provided that all recommendations listed in the present report are implemented and respected during the rollout and utilization of the new functionality.

The rollout of AFIS functionality should be preceded with the selection of the most appropriate special quality check tools (as required by Article 22(a)) and with the production of detailed statistics on consultations related to persons as carried out currently in SIS-II.

Main findings and Recommendations

The JRC has listed 19 recommendations to support successful deployment and use of an AFIS in SIS-II. The recommendations cover the following topics: national expertise and best practice; selection of appropriate formats to collect, exchange and process data; production of statistics; identification of appropriate architecture options; application of rigorous procedures for biometric enrolment; selection of measures to foster quality; definition of use-case scenarios and introduction of regular performance evaluation actions.

Related and future JRC work

The JRC has already conducted a study on the quality of children's fingerprints[4]. This work was based on a dataset provided via a collaboration with the Portuguese Authorities. An extension of this collaboration has given access to a much larger dataset which will allow the JRC to conduct further quality-related experiments on fingerprint quality comparison among significant age groups (i.e. children, adults, elderly), which could be of relevance for the future of SIS-II and in particular its AFIS.

JRC will launch, in 2016, a competition on AFIS performance which could be adapted to the SIS-II context with the active support of the Member States and could provide useful results for future SIS-II AFIS deployment.

Quick guide

A biometric system is essentially a pattern recognition system that makes use of biometric traits to recognize individuals. An AFIS is an automated identification biometric system which searches whether specific fingerprints are present in a large database of fingerprints. If the search is positive, the results will be the list of all possible individuals whose fingerprints match the specific fingerprints.

[4] Fingerprint Recognition for Children (2013), DOI 10.2788/3086, EUR 26193 EN, http://publications.jrc.ec.europa.eu/repository/handle/JRC85145

List of recommendations

RECOMMENDATION 1: Need for complementary statistics

- We recommend that, following a consultation with the EDPS by the Commission, eu-LISA identifies the best possible ways to include in its statistic annual report the number of consultations per year related to persons. In order to complement this assessment at central level, we also recommend that Member States report annually on the number of consultations related to persons that have been carried out on their national copies and, whenever possible, on the context of these consultations (e.g. at the police office, at border check).

RECOMMENDATION 2: Promotion of best practices

- We recommend that the expertise acquired during the development and management of national AFIS is appropriately applied to the SIS-II AFIS deployment and that best practices identified at national level are further fostered.

RECOMMENDATION 3: Common exchange standard

- So far, NIST containers, as required by the SIRENE Manual and the best practice guide from Interpol, seem to provide an appropriate basis regarding the exchange of fingerprint data. We recommend that an automatic check for their mandatory and complete implementation should be developed in order to appropriately support the deployment of the SIS-II AFIS functionality.

RECOMMENDATION 4: Prüm and SIS-II complementarity

- A need for clarification between the functionalities of Prüm system and of a future SIS-II AFIS was strongly identified during the visits. We recommend that this need is addressed.

RECOMMENDATION 5: Dedicated sub-systems

- In order to better respect the different business cases envisaged for a SIS-II AFIS, we recommend to consider in the design of such a system the use of dedicated sub-systems for each category of query.

RECOMMENDATION 6: High-quality enrolment process

- We recommend that, whenever a data subject is available, that is, in most of the cases, the enrolment phase should favour the use of live-scan devices and be conducted under the control of experienced operators, as is usually the case in a law enforcement context. This should result in the production of a high-quality ten print card containing both rolled and flat data.

RECOMMENDATION 7: Storage of multiple datasets

- We recommend to envisage the storage of multiple datasets (e.g. four datasets) for a SIS-II AFIS to support a composite matching strategy. As long as it is clearly established that the datasets belong to a same person, a composite check would be the result of multiple datasets associated with a single alert or datasets belonging to several alerts, which should already benefit of links established in accordance with Article 52 of the SIS-II Decision.

RECOMMENDATION 8: Controlled transfer of datasets

- We recommend that SIS-II AFIS accepts fingerprint datasets produced via other systems, as long as the parameters of these systems are kept in the dataset included in the alert. NIST containers offer the possibility to keep several quality scores issued by different systems.

RECOMMENDATION 9: Quality of capture points

- **Supervision by an operator.** Adequate operator training is recommended, as supervision of biometric acquisition is a repetitive task and requires additional attention in the case of centralised enrolment stations. The aim is to avoid tiredness and boredom adversely affecting the process.
- **Adequate sensor.** We recommend to use performant fingerprint sensors (e.g. in size and resolution), offering also enhanced capabilities to acquire low-quality sources. Whenever possible live-scan devices should be favoured for capturing fingerprints.

- **Enhanced graphic user interface (GUI).** We recommend that capture points have large displays and provide real-time feedback of acquired data.
- **Proper user interaction.** The enrolment process should be user-friendly with clear procedures which are properly explained. The use of good ergonomics should support better acquisition practices.
- **Adequate environment.** The acquisition environment should be appropriate in terms of illumination, temperature and backgrounds both for the subject and the operator. These elements are recommended mainly for fixed stations but similar considerations are instrumental as well for mobile stations.
- **Sensor maintenance.** There should be regular and systematic cleaning of the enrolment stations to avoid "ghost fingerprint" effect, especially in the case of consultation processes taking place in heavily used check points.

RECOMMENDATION 10: Quality assessment algorithms

- **Adherence to standards.** We recommend to include in a SIS-II AFIS the results of the quality metrics algorithm used locally by Member States as well as the results of the use of standard quality metrics such as NFIQ and NFIQ-II. These two results will complement those provided by the quality metrics algorithm of the SIS-II Central AFIS functionality. All three results can be added in a single NIST container, as for ANSI/NIST-ITL 1-2000 standard (see Recommendation 3 above).
- **Corrective actions.** We recommend to implement an acquisition loop/recapture procedure to be carried out until satisfactory quality prints have been obtained. This procedure should contemplate alternative acquisition processes, according to the sample quality, and should include human intervention, where appropriate.

RECOMMENDATION 11: Quality of identification systems

- **Quality-based processing.** In addition to the standard algorithms and tools used for fingerprint identification, we recommend the use of supplementary tools such as alternative feature extraction functions and process-specific matching algorithms.
- **Quality based fusion.** We recommend to combine different samples so as to be able to conduct composite checks. Should the revision of the SIS legislation allow this option at a later stage, it would be interesting to combine different biometric traits (e.g. multimodal biometric matching system) to improve identification results.
- **Template substitution/update.** When generating templates for an AFIS, we recommend to select best stored samples.
- **Monitoring.** We recommend to produce statistics for each type of applications, sites, devices, and operators, so as to obtain a user-scanner learning curve and propose training measures, as needed.

RECOMMENDATION 12: Children cases

- The majority of alerts on missing persons are related to minors. We recommend that a SIS-II AFIS includes the possibility to tune the matching process towards such cases, in particular, when fingerprint data in the alert are more than two years old.

RECOMMENDATION 13: Quality check central service

- We recommend that an automated central service is offered to Member States to check fingerprint quality against the SIS-II AFIS quality metrics. A similar service exists already for the VIS with a response time of less than 30 seconds. Such a system would provide a significant additional feedback to the operator on the quality of the fingerprint dataset being acquired.

RECOMMENDATION 14: Reporting on lower quality fingerprint card

- We recommend to record when a dataset, which is proposed for enrolment or for addition in an alert, has not the quality level required for the SIS-II AFIS either in an alert or in the dataset card

itself. Such a record would take place, for instance, when a ten print card is produced from a system that acquires flat prints only (e.g. the VIS).

RECOMMENDATION 15: Integrity of the database

- We recommend the use of best practices to reduce the risk of inconsistency or erroneous data, including fingerprints, recorded in the database. Efficient methods should be designed to find, mitigate, correct or prevent the occurrence of such issues. These methods are of organizational and technical nature. As an example, during a two print consultation, a cross-check should be conducted on the two fingers. In case of a match between a left index and a right index stored in the AFIS, a message should be sent to the Member States which has introduced the alert.

RECOMMENDATION 16: Consultation

- **Enhanced resolution (1000dpi).** We recommend to give the possibility to store fingerprints at a 1000dpi resolution to those Member States that have already upgraded their scanners at that resolution.
- **Flat and rolled fingerprints.** We recommend that Member States should be allowed, for consultation only, to limit fingerprint collection only to flat prints. Member States have already implemented this option at national level since it is a faster method compared to using both flat and rolled data.
- **Two prints fast check.** We recommend to offer the possibility to carry out quick consultations. Such quick consultations are required in situations such as first line border control or on-the-spot street checks. The result of these consultations should be a hit/no hit reply which can trigger, in case of a hit, a second line control check.

RECOMMENDATION 17: Appropriate response times

- We recommend that the SIS-II AFIS complies with the following three response times, which are at this stage only indicative and tend to reflect the discussion which took place with Member States: (a) A very short response time (i.e. below 30 seconds) should be expected from a first line of border control check or a mobile check by a field law enforcement officer. (b) A medium response time (i.e. below five minutes) should be expected from a second line control check at the border or at a consular post (e.g. in the course of a VISA application). (c) A longer response time (i.e. up to ten minutes) could be tolerated for law enforcement consultations taking place at a police station, especially in the case of latents.

RECOMMENDATION 18: Queries priority

- We recommend the definition of priority levels for processing queries in order for a SIS-II AFIS to manage better the workload of the system.

RECOMMENDATION 19: Performance benchmark

- Considering that carrying out an in-depth performance evaluation is time and resource consuming, we recommend that such evaluations are planned already in the development phase of a SIS-II AFIS and are performed at the time of its rollout, as well as, every four years or every time a major update of the matching system is installed, whichever comes first.

This page is intentionally left blank.

Table of contents

List of tables

List of figures

Main acronyms and abbreviations

AFIS	Automatic Fingerprint Identification System
DHS/OBIM	Department of Homeland Security/ Office of Biometric Identity Management
dpi	Dots (pixels) per inch
EER	Equal Error Rate
EP	European Parliament
EU	European Union
EC	European Commission
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FRR	False Rejection Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FTA	Failure to Acquire
FTE	Failure to Enrol
ISO	International Organization for Standardization
MS	Member State
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology
ROC	Receiver Operating Characteristic
RRR	Record Rejection Rate
SIS	Schengen Information System
TAR	True Acceptance Rate
US	United States of America
VIS	Visa Information System

Acknowledgements

This report was prepared out by members of the team in charge of the "Biometric and Border Management (BBM)" project, working at the Digital Citizen Security Unit of the Institute for the Protection and Security of the Citizen, Joint Research Center. The study would not have been possible without the help, dedication and active involvement of a number of people working in different institutions all over Europe and beyond. With our apologies to all those people who actively contributed to the study and are not explicitly mentioned hereafter, the authors would like to give a special recognition to:

DG JRC and DG HOME

We would like to thank the following colleagues from the European Commission for their determinant support, comments and contribution:

Günter Schumacher, Jean-Pierre Nordvik, DG JRC IPSC Digital Citizen Security Unit

Zsuzsanna Felkai-Janssen, Richard Rinkens, Rob Rozenburg, Michael Flynn DG HOME Information Systems for Borders and Security unit

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)

We would like to thank all the colleagues from eu-LISA who provided us on a regular with basis key information and explanations on the operational management of the three large scale IT systems currently working in Europe, namely EURODAC, Visa Information System, and Schengen Information System II.

EU Member States and United States of America Authorities

We would like to express our gratitude for the representatives of the nine EU Member States visited and contacted during the fulfilment of the study: Austria, Finland, France, Germany, Italy, Netherlands, Portugal, Romania and Spain.

We would like as well to thank the USA representatives from the National Institute for Standards and Technology (NIST), Department of Justice, Federal Bureau of Investigation (FBI) and Department of Homeland Security – Office of Biometric Identity Management (DHS-OBIM) for their great hospitality, openness and full cooperation.

External experts Board

We would also like to thank the renowned international experts who joined the external scientific board of the study for reviewing its results and conclusions:

Christophe Champod, Université de Lausanne, Faculté de droit, des sciences criminelles et d'administration publique, Ecole des sciences criminelles

Julian Fierrez, Universidad Autonoma de Madrid, Escuela Politécnica Superior, Biometric Recognition Group - ATVS

Olaf Henniger, Abteilung Identifikation und Biometrie, Fraunhofer-Institut für Graphische Datenverarbeitung IGD

Davide Maltoni, Università di Bologna, Facoltà di Ingegneria e Scienze Informatiche, Biometric Systems Laboratory (BioLab)

Didier Meuwly, Netherland Forensic Institute, Special Chair in Forensic Biometrics - University of Twente

This page is intentionally left blank.

1 Introduction

In September 2014, DG HOME and the JRC agreed on Administrative Arrangement JRC 33516-2014 NFP aiming to study the readiness and availability of Automatic Fingerprint Identification System (AFIS) technologies for their introduction in the second generation Schengen Information System (SIS-II).

AFIS technology has been ready and available for many years and, as will be described later in the study, it has been implemented and used in numerous databases. However, the level of readiness and availability have to be assessed in the context of the unique situation and characteristics of SIS-II which present a series of technical and organisational challenges requiring appropriate and customised solutions.

The objective of this JRC study is therefore to provide a report supporting the decision-making process on whether fingerprint identification technology is mature enough for inclusion in SIS-II. This report presents the main findings of the JRC study together with options and recommendations for successful implementation of this AFIS functionality. The operational implementation of such functionality will require an additional dedicated study providing the detailed specifications emanating from the recommendations and options selected from the JRC study. In Annex 1 a series of technological concepts and definitions related to AFIS is provided in order to facilitate the reader's task.

1.1 Policy, technical and legal contexts of SIS-II

The second generation Schengen Information System (SIS-II) entered into operation on 9 April 2013. Its original version, SIS-I was the first so-called large-scale IT system launched by the EU Member States in 1995 and was followed by EURODAC (asylum seekers' database) in 2003 and the Visa Information System (VIS) in 2011. Created as a compensatory measure for the abolition of internal border checks within the Schengen area, SIS was established with two intentions: to contribute to law enforcement cooperation between the Member States and to support external border control.

SIS-II enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. A SIS-II alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. Among the 61 million of alerts stored in SIS-II, 1.43% are related to persons (around 800 000). An alert always consists of three parts: firstly a set of data for identifying the person or object in the alert, secondly a statement why the person or object is sought and thirdly an instruction on the action to be taken when the person or object has been found.

The quality, accuracy and completeness of the data elements enabling identification are the key conditions for the success of SIS-II. For alerts on persons the minimum data-set is name, sex, a reference to the decision giving rise to the alert, and the action to be taken. When available, photographs and fingerprints must be added in order to both facilitate identification and avoid mis-identification.

SIS-II consists of three major components: a central system, national systems which may contain a synchronised copy of the data in the central system, and a communication infrastructure (network) between the central system and the national systems. An alert which is entered in SIS-II in one Member State is transferred in real time to the central system. It then becomes available so that authorised users can carry out queries in the database by entering search data on persons and objects. A detailed description of SIS-II and the five types of alert related to persons which can be created is available in Section 7 of this report.

In the case of alerts related to persons, SIS-II offers the possibility to process biometric data, as is already the case with EURODAC and the VIS. It is foreseen according to Articles 22(c) of SIS-II Decision[5] and Regulation[6] that SIS-II may also be used to *identify* a person on the basis of his/her fingerprints, a functionality which will require the implementation of an Automatic Fingerprint Identification System (AFIS) "*once it becomes technically possible*" and when the Commission has presented "*a report on the availability and readiness of the required technology on which the European Parliament is consulted*".

According to Article 22.b of the SIS-II legal framework, currently, fingerprints and photographs can be used only to *confirm and verify* the identity of a person who has initially been identified on the basis of alphanumeric data (e.g. name and date of birth). When attached to the alert concerning the person, these biometric data are manually processed in order to conduct an identity verification.

These biometric data can be added to alerts only after a quality check as required by Article 22(a). This quality check should be defined through a comitology procedure. The SIRENE Manual annexed to a Commission Decision[7] describes the way these data should be attached to an alert. The Manual contains detailed rules for the exchange of supplementary information. Supplementary information is information not stored in SIS-II but connected to SIS-II alerts, which is to be exchanged between Member States.

In addition to the centralised large-scale IT systems, EU Member States have developed, under the umbrella of the Prüm Treaty[8] and later in the context of the Decision 2008/615/JHA[9], the possibility to query national criminal AFIS. The Decision provides for the automated exchange of DNA, fingerprints and vehicle registration data, as well as other forms of police cooperation between the 27 EU States. A brief comparison between the Prüm mechanism and SIS-II can be found in Annex 2. The Prüm mechanism was not initially identified as part of the policy context of the study but it has been highlighted and discussed by the Member States visited.

1.2 Technology: readiness and availability

According to the Horizon 2020 EU Research and Innovation Framework Programme the readiness and availability of a given technology is assessed using nine different levels (Technology Readiness Levels, TRL):

- TRL 1 – basic principles observed,
- TRL 2 – technology concept formulated,
- TRL 3 – experimental proof of concept,
- TRL 4 – technology validated in laboratory,
- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies),
- TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies),
- TRL 7 – system prototype demonstration in operational environment,
- TRL 8 – system complete and qualified,
- TRL 9 – actual system proven in operational environment.

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0004:EN:PDF

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0334&from=FR

[8] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010900%202005%20INIT

[9]http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008D0615&from=EN

As will be explained in this report, although AFIS technology has reached TRL 9[10], with multiple large-scale systems already deployed and working worldwide, each operational scenario has its own specificities. As such, the successful application of a certain technology to a given specific use-case and environment, does not necessarily guarantee the same level of success when those operational conditions are changed.

In particular, for AFIS technology to achieve the expected level of performance, there are certain parameters that have to be taken into account. Probably, the most important of these features is the **accuracy** that can be expected from AFIS. Unfortunately, the answer to the question of how accurate current systems are is not straightforward, as it largely depends on the data (i.e. fingerprint samples) a system will have to deal with and, more particularly, with the **quality** of that data. Furthermore, depending on the **use-cases** defined for such AFIS, a different level of accuracy may be acceptable and/or expected.

This report describes current AFIS technology and clearly states the challenges faced by this type of system, giving a series of recommendations on how to best face these challenges so that the outcome of the eventual integration of AFIS technology in SIS-II is successful.

1.3 Methodology followed for conducting the study

The study was conceived as a three step task with some slight overlap between the steps:

- STEP 1: Wide collection of information regarding AFIS technology.
- STEP 2: Synthesis of the information obtained from multiple sources.
- STEP 3: Producing the report.

STEP 1 was the most important and, as such, the most time and resource consuming. This step provided all the necessary information for the JRC analysis and eventually led to the current report. This information was collected over five phases, each of them involving different sources. These phases are detailed in the next sections.

1.3.1 Phase 1: Analysis of the state of the art in AFIS technology

Relevant bibliography and scientific literature were extensively reviewed in order to consolidate and complement JRC knowledge and obtain an initial solid overview of the main features and challenges of AFIS. Such a study of the AFIS field was necessary in order to prepare the set of visits and consultations carried out in the next phases.

1.3.2 Phase 2: Consultation with national AFIS

The final users of a future AFIS in SIS-II will be the competent authorities of the different Member States (MS), such as police and border guards. During the design process of such an AFIS, it is therefore extremely important to know the operational contexts in which MS are using their national AFIS, the similarities and differences between them, as well as their needs.

Following the rationale described above and in order to address the objective of assessing "*the availability and readiness of the required technology*" for the inclusion of an AFIS in SIS-II, the JRC first contacted and visited nine EU Schengen Member States' law enforcement entities (France, Germany, Italy, the Netherlands, Austria, Portugal, Romania, Spain, Finland). The objectives of these exchanges were threefold:

- Learn which technologies these countries have implemented in order to operate a national AFIS;

[10] Similar classification and approach can also be found in the report "Best Practices in Testing and Reporting Performance of Biometric Devices" by Wayman and Mansfield from 2002. http://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=59&dno=9&fseq=1

- Identify which best organisational and procedural techniques they have developed;
- Describe the remaining challenges they face.

These visits also led to better understanding of how and in which cases Member States are already using their national AFIS, SIS-II or any other AFIS (e.f, EURODAC, Prüm, Interpol). The visits also gave an opportunity for the JRC to collect the possible expectations those authorities might have regarding the introduction of AFIS functionality in SIS-II.

The visits to the nine MS were complemented with a visit to the United States of America, the host of some of the biggest and most advanced AFIS, presenting broad similarities with the objectives and expected use of the SIS-II AFIS.

With the support of DG HOME, the JRC first sent an introductory letter to the targeted countries asking for a possible visit to their National AFIS and presenting the overall objectives of the study. All countries replied positively to the JRC letter, provided the technical contact for the visit and actively cooperated in its organisation.

Those visits were also facilitated by the preparatory work done by DG HOME during the SISVIS committee meetings during 2014 and the preliminary questionnaires related to the possibility of introducing AFIS submitted to the members of this committee.

An outline of the envisaged technical exchange was sent to the countries prior to the visit (see annex 3). This outline aimed to inform them by providing a list of preliminary questions regarding the different technical fields the JRC wished to explore during the visit. Each visit focused on the following subjects:

- The use-cases in which fingerprints are processed;
- A technical description of the national AFIS;
- The management of the life cycle of fingerprint data in their system;
- The possibility to have a live demonstration of the use of the AFIS.

The JRC visits targeted national AFIS used in the context of criminal matters and managed by national police forces. However, for each visit, authorities in charge of border management (also using the national AFIS) were included and participated in the presentations and discussion.

At the beginning of each visit, the JRC gave an introduction and proposed an agenda divided into three main steps:

- The National AFIS;
- Current and future uses of SIS-II;
- Use of other EU/international system such as Prüm, INTERPOL, etc.

The visits were conducted by two JRC scientific officers. This team of two was necessary to cope with the very rich and intensive discussion offered by the visited countries.

At the end of each visit, the JRC provided the timescale of the study and invited participants to review the final draft of the present report. The timeline and most relevant information concerning the visits are summarized in Table 1. Summary of the key information concerning the visits to the institutions managing the national AFIS in different countries.

COUNTRY	DATE	INSTITUTION	COMMENTS
Finland	3/12/2014	National Police Board	Other institutions represented: National Bureau of Investigation Ministry of Foreign Affairs Ministry of the Interior
Austria	16/12/2014	Criminal Intelligence Service Austria	
Portugal	13/01/2015	Laboratorio de Policia Cientifica	
Romania	03/02/2015	National Police Forensic Institute	
Netherlands	10/02/2015	National Police Forensic Service	Other institutions represented: Ministry of Defence
Spain	16/02/2015	Policia Nacional Policia Cientifica	Other institutions represented: Ministerio de Interior
France	27/02/2015	Police National Technique et Scientifique	
Italy	31/03/2015	Polizia di Stato	
United States	09-13/03/2015	US National Institute for Standards and Technology (NIST) Department of Justice Federal Bureau of Investigation Department of Homeland Security – Office of Biometric Identity Management	
Germany	22/07/2015	Federal Criminal Police Office Wiesbaden ZD 23 - AFIS	Conference-call

Table 1. Summary of the key information concerning the visits to the institutions managing the national AFIS in different countries.

1.3.3 Phase 3: Consultation with eu-LISA

The visit on 19 January 2015 to the European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) allowed the JRC to obtain an accurate picture of the central part of the EU AFIS already in production such as the Visa Information System (VIS) and EURODAC. It also provided a detailed description of the SIS-II central system and its reporting capability. This visit was followed by a series of exchanges and conference calls with the officers respectively in charge of SIS-II, VIS and EURODAC until the end of the study, providing the latest up-to-date statistics of those systems when available.

1.3.4 Phase 4: Consultation with AFIS vendors

The information collected from authorities already using AFIS was completed by discussions with the vendors of such technology. This also allowed the JRC to have a better understanding of the deployment challenges faced by the actual designers of such systems.

Although numerous companies offer AFIS in multiple domains, most of them are integrators and do not themselves develop AFIS solutions. In the light of the discussions with the nine national authorities visited, Morpho[11] and 3M[12], which provided AFIS to those authorities, were consulted.

1.3.5 Phase 5: Consultation with external review board of experts

In order to review the results and conclusions established in this report, an External Review Board comprised of Davide Maltoni (IT), Olaf Henniger (DE), Julian Fierrez (ES), Didier Meuwly (NL) and Christophe Champod (CH) was set-up. An introductory meeting was organised at the end of April 2015. The final draft version of the report was then submitted to them at the end of July 2015. The five experts presented their review, comments and suggestions in the course of a meeting held in Ispra on 26 and 27 of August 2015.

1.4 Structure of the report

The methodological approach adopted by the JRC for the analysis was to explore and assess the main characteristics and challenges of AFIS in general and then apply these identified elements to the specific context of SIS-II and suggest recommendations to appropriately address them. Accordingly, the JRC report contains two main parts:

- **PART I** sets the scene on the current status of AFIS technology. It introduces the key parameters that define the readiness of a given technology, such as its performance. This part also presents some general concepts regarding the quality of the data which is a factor that has a key impact on the performance of AFIS. The reader will also find in this part a summary of the main characteristics of some of the most important large-scale AFIS already working worldwide, as well as a summary of the key features of an AFIS.
  As a wrap-up, PART I finishes with a section dedicated to the main challenges faced by AFIS designers when putting in place such new large-scale systems. All these challenges have been extracted from the large amount of information provided by the different sources consulted during the preparatory stages of the report (i.e. bibliography, Member States, vendors, eu-LISA, and external experts' board).
- **PART II** focuses first on SIS-II as it is implemented today, presenting some facts related to different statistics concerning the system such as the number of alerts, the actual size of the database, number of queries, current architecture, expected use-cases or relevant legislation. After this initial presentation of the system, PART II builds on the initial scene, concepts and key features for the AFIS technology introduced in PART I and on the specificities of SIS-II, to give a series of recommendations, suggestions and options on how each of the challenges presented at the end of PART I could be potentially dealt with in the case of SIS-II in order to successfully implement an AFIS functionality in the most effective way possible.
  PART II finishes with a more prospective look into the future giving some possible actions (still not contemplated by the current legislation) that could be undertaken in the years to come in order to further improve the accuracy, flexibility and ultimately the added-value offered by SIS-II to the Member States.

1.5 Audience of the report

Although the report has been conceived as a self-contained document to be read by a wide general audience, technical terms and aspects related to biometric technology are discussed in the different sections. Therefore, for those readers who are laymen in biometrics, it is strongly recommended to first read the final annexes (and references therein) where some basic technical concepts are

[11] http://www.morpho.com/

[12] http://solutions.3m.com/wps/portal/3M/en_US/Security/Identity_Management/

introduced. This initial reading can facilitate a better grasp of the implications and findings of the report.

This page is intentionally left blank.

PART I: OVERVIEW OF AFIS TECHNOLOGY

As already mentioned in Section 1.2, one of the most important features, if not the most important one, that defines the readiness and availability of AFIS, is accuracy. This accuracy is deeply impacted by the quality of the data (i.e. fingerprint impressions) that the AFIS has to deal with. In addition, both performance and quality depend on the different use-cases in which the AFIS will be deployed and used.

PART I of this report is structured according to these three key aspects: accuracy, quality and use-cases. First, some general notes about AFIS performance evaluation are provided. Second, the concept of biometric quality and its impact on the performance of biometric systems is introduced focusing always on the fingerprint biometric trait. Third, we present different use-cases in which AFIS are utilized by the end-users of a potential SIS-II AFIS (i.e. national police forces of the different MS), together with the most significant operational differences observed during our visits to the Member States. Fourth, we describe some of the large-scale IT systems already in production today.

In the final section of PART I, we list and summarise the main challenges faced by current AFIS technology which have to be taken into account when considering the introduction of such functionality in a new large-scale system.

2 AFIS Accuracy Evaluation

Considered as the main pillar for determining the readiness and availability of AFIS technology, accuracy constitutes the main focus of the present section. This dimension is tackled through an analysis of the key aspects to be taken into account for the assessment of error rates and a review of the most significant independent evaluation campaigns conducted so far.

Although the most important, accuracy represents only one of the parameters which determine the performance of an AFIS. Other performance parameters that are not considered in this section (or only from a very general perspective) are for example: matching speed, computational efficiency and response time or template size.

Objective accuracy evaluation of biometric systems is not a straightforward task. In an ideal situation, one would like to assess the application-independent accuracy of a recognition system and be able to predict its real operational accuracy in any context. In this ideal scenario, rigorous and realistic modelling techniques simulating data acquisition and matching processes are the only way to obtain and extrapolate the accuracy evaluation results. More research effort is still required to further address this problem.

In the meantime, performing comparative evaluations on specific scenarios is the norm. Until many aspects of biometric recognition algorithms and application requirements are clearly understood, comparative, empirical, application-dependent evaluation techniques will be predominant and the evaluation results obtained using these techniques will be meaningful mainly for a specific database in a specific test environment and a specific application. Another disadvantage of empirical evaluation is that it is expensive to collect the data for each evaluation, complement them with the ground truth metadata and implement additional data protection measures so as to fulfil the obligations related to this new purpose. It has to be highlighted that objectively comparing the evaluation results of two different systems, tested under different conditions, presents limitations in the relevance of the comparison.

Depending upon the data collection protocol, the accuracy results can vary significantly from one benchmark to another. Within the biometric recognition context, a benchmark is defined by a database and an associated testing protocol. Generally the protocol defines (at least) the subsets of images that can be used for training and testing, the pair of images that have to be compared, the performance metrics to be used and how they must be computed.

Below, a summary of the most important independent evaluation campaigns that have been performed in fingerprint recognition will be presented. It is important to note that, as pointed out above, any effort to assess the general performance of any biometric system in verification or identification transactions must be undertaken with care. The accuracy and overall performance of any method or system will depend on multiple factors which are difficult to model or to objectively quantify, including the quality of data input (and hence the sensor and feature extraction algorithms), the specific matching algorithms used, the population being assessed and in the case of identification from a database, the number of entries to be searched. Thus, the results presented in this section should be assessed with these caveats as they are valid only for the use-cases and situations in which the testing described was carried out. Performance expectations in other scenarios based on these results cannot simply be assumed.

Bearing in mind the previous caution, the results obtained in a performance evaluation can be useful for environments similar to the one envisaged by the data used and, if properly analysed, they can reveal important factors to consider in other environments (and most importantly: how to consider such effects). What is important to emphasize is that, in those cases where the scenario under study is not identical to the one defined in a benchmark, the results previously obtained in that benchmark should be carefully interpreted and probably adapted, e.g. previous FVC and NIST evaluations disclose

very important information to be considered as a basis for the proposed development of an AFIS in SIS-II (a basis that can be fine-tuned with specific and more targeted benchmarks using real SIS-II data).

Therefore, the series of evaluations presented below, can help to provide an overall picture not only of the evolution of the state of the art over the last 15 years but also on the performance capabilities of fingerprint recognition systems today. The most significant independent evaluation campaigns that have been carried out so far in fingerprint recognition are:

- the two NIST Fingerprint Vendor Technology Evaluations: FpVTE 2003 and FpVTE 2012,
- the NIST Evaluation of Latent Fingerprints Technologies (ELFT), which has had different phases between 2007 and 2012,
- the NIST Proprietary Fingerprint Template Evaluation (PFT) which has had two phases, one from 2003-2010 and a second which started in 2010 and is still ongoing,
- the NIST Minex initiative which has had different stages between 2004 and 2015,
- the five Fingerprint Verification Competitions (FVC), which took place in 2000, 2002, 2004, 2006 and the continuing over time FVC-OnGoing.

All these initiatives will be briefly described in the following sections. Those that are most relevant to the SIS-II are the NIST FpVTE and the NIST ELFT, as they assess the accuracy of AFIS, while the rest deal with the accuracy of fingerprint verification systems (for a clarification on the differences between biometric systems working on “identification” and “verification” we refer the reader to Annex 1).

In particular, the closest evaluation to the SIS-II system, both in terms of type of fingerprint data and size of the database, is the NIST FpVTE 2012. Even if results cannot be directly extrapolated, this evaluation can be considered as a good estimation of the accuracy that can be expected from AFIS technology in the SIS-II operational environment.

The two most relevant metrics used in these evaluations to assess performance were:

- False Positive Identification Rate (FPIR): FPIR is the fraction of the non-mated searches (i.e. searches of an identity that is not in the database), where one or more enrolled identities are returned at or above a certain threshold.
- False Negative Identification Rate (FNIR): FNIR is the fraction of the mated searches (i.e. searches of an identity that does exist in the database), where the enrolled mate is outside the ranked list of identities returned by the system or that the comparison score is below a given threshold.

For further details on these and other metrics used to evaluate the accuracy of AFIS, the reader is referred to Annex 1. Also, please refer to Annex 1 for further details on terms such as: ten print searches, latent fingerprints, live-scanned/inked fingerprints, flat/rolled fingerprints.

2.1 NIST Fingerprint Vendor Technology Evaluations (FpVTE) 2003 and 2012

Following the path started by the successful Fingerprint Verification Competitions (FVC) organized by the University of Bologna for the first time in 2000, in 2003 NIST conducted the first Fingerprint Vendor Technology Evaluation (FpVTE): an independently administered technology evaluation of fingerprint matching, identification, and verification systems.

FpVTE 2003 was designed to assess the capability of fingerprint systems to meet requirements for both large-scale and small-scale real world applications. FpVTE 2003 consisted of multiple tests performed with combinations of fingers (e.g. single fingers, two index fingers, four to ten fingers) and different types and qualities of operational fingerprints such as flat live-scan images from visa applicants, multi finger slap live-scan images from present-day booking or background check systems or rolled and flat inked fingerprints from legacy criminal databases).

The contest was entered by 18 different private biometric companies including some of the biggest players at international level such as Morpho or 3M-Cogent. A detailed description of the competition together with all the results may be found in [NIST2004].

In 2012, NIST launched a new Fingerprint Vendor Technology Evaluation (FpVTE) with two main goals. The first was to assess the current capabilities of matching algorithms using operational datasets with several million subjects. The second was to evaluate different operational considerations that could impact matching accuracy. These considerations included number of fingers used, data types (live-scan, single finger capture, slap capture requiring segmentation and rolled), number of enrolled subjects and matching speeds.

As in the previous contest, all the main vendors in the fingerprint recognition field at international level took part in the competition. This is, so far, the latest fingerprint technology evaluation carried out and therefore, the one that can give a clearer picture of current AFIS capabilities. As such, a brief summary of the results obtained in the competition is given in Table 2 Result of the best performing algorithm in the tasks of: single index identification, 2-indexes identification and ten finger identification. where the size of the search database *N* is given in parenthesis as one of the critical parameters in the evaluation of AFIS accuracy [Jarosz2005]. For a full description of all the scenarios considered in the competition and a detailed analysis of the results we refer the reader to [NIST2014].

	1-index ident.	2-index ident.	10-finger ident.
FNIR @ FPIR=0.1%	1.97% (*N*=100.000)	0.27% (*N*=1.600.000)	0.1% (*N*=5.000.000)

Table 2 Result of the best performing algorithm in the tasks of: single index identification, 2-indexes identification and ten finger identification.

The figures show the False Negative Identification Rate (FNIR) at a False Positive Identification Rate of 0.1%. N indicates the size of the search database which is a critical factor in AFIS accuracy assessment. For further details on the evaluation protocol used we refer the reader to [NIST2014]. The definitions of FNIR and FPIR as well as other relevant information regarding AFIS accuracy assessment can be found in Annex 1.

2.2 NIST Evaluation of Latent Fingerprints Technologies (ELFT)

The ELFT initiative started in 2006 with the organization by NIST of a preliminary workshop. The main findings can be consulted in [NIST2006]. The workshop led, in 2007, to the organization of the first ELFT evaluation, which aimed to assess the core capabilities of current automatic latent matching algorithms. The evaluation consisted of two tests, run in a "lights-out" environment. "Lights-out" refers to a fully automatic scenario with no human intervention. The two tests were termed Phase I and II. Phase I was a proof of concept test, the main purpose of which was to demonstrate integrity of the software in a lights-out environment. During Phase I the software would demonstrate: 1) automated feature extraction from latent images; 2) the ability to match these features against enrolled ten print backgrounds and 3) generation of candidate lists. Phase II then employed a larger database to quantify the achievable performance for automated searches.

All the tests and results carried out in Phase II are detailed in [NIST2009], where the best performing algorithm over 500 dpi images obtained a Rank 1 accuracy of 96.4% and a Rank 10 accuracy of 97.2% over a search database of *N*=100.000 identities.

The ELFT initiative continued in 2009 with the organization of a second workshop and with the announcement of a second evaluation in a "semi lights-out" environment, that is, where some human intervention is allowed but the final identification task is fully automatic. The main purpose of the evaluation was to assess the accuracy of latent matching using features marked by experienced human latent fingerprint examiners. A key result of the test was to determine when human minutiae mark-up is effective. As human mark-up is expensive in terms of time, effort and expertise, there is a

need to know when image-only searching is adequate and when the additional effort of marking minutiae and extended features (e.g. sweat pores, core, delta) is appropriate.

The final report of this second 2009 ELFT evaluation was published in [NIST2011]. Unfortunately the data used in 2006 ELFT-Phase II and that used in 2009 ELFT-Extended Feature Sets were totally different and therefore the results are not comparable. In the 2009 human-aided evaluation, the Rank 1 accuracy of the best system was 62.2% over a search database of *N*=100.000 identities (see Annex 1 for a complete definition of Rank 1 accuracy).

Additionally, continuing this line of latent performance evaluation, in 2013 NIST made public a presentation by the Federal Bureau of Investigation (FBI) which gives selected statistics on State and Federal Agency latent fingerprint searches. The document also discusses methods for improving performance (individualization) for latent searches and covers steps toward greater automation in the future, such as increased reliance on image-only searches [FBI2013].

2.3 NIST Proprietary Fingerprint Template Evaluation (PFT)

The National Institute of Standards and Technology's Proprietary Fingerprint Template evaluation is an ongoing program to measure the performance of fingerprint matching software by utilizing vendor proprietary fingerprint templates. There have been two phases to the PFT evaluation:

- The original PFT evaluation (which is no longer accepting SDKs for evaluation and which ran between 2003 and 2010) which only reported the matching algorithm's accuracy. Most of the results of this initial phase are reported in [NIST2005].
- The newer PFTII evaluation (which is currently accepting SDKs for evaluation) also reports matcher accuracy information and, in addition, will also report on other useful information such as template extraction times, template size information and matcher timings. PFTII will use both two finger and ten finger datasets to report results on slap-to-slap, slap-to-roll, and roll-to-roll matching. PFTII continues to be only a one-to-one verification evaluation, it does not report one-to-many matching results (if needed, see Annex 1 for a detailed description between “one-to-one” and “one-to-many” matching).

These evaluations are intended to assess the core algorithmic capability of the technology to perform one-to-one verification. These evaluations assess the accuracy of end-stage matchers, that is, the computationally expensive algorithms used in the very last stages of one-to-many AFIS searches. This evaluation is not necessarily representative of a provider's capability to field large-scale identification technologies, because AFIS engineering requires trade-offs between efficiency, cost, accuracy and other resources, and usually exploits multi-stage matching techniques to expedite search. As such, high accuracy from these evaluations does not automatically imply that a provider has the capability to provide a full-scale AFIS installation.

2.4 NIST Minutiae Exchange (MINEX)

The approval of the International Committee for Information Technology Standards (INCITS) 378 fingerprint template standard created the possibility of a fully inter-operable multi-vendor marketplace. As a result of this standard, NIST launched, in 2004, the MINEX evaluation. The purpose of the "Minutiae Interoperability Exchange Test (MINEX 04)" was to determine the feasibility of using minutiae data (rather than image data) as the interchange medium for fingerprint information between different fingerprint matching systems. MINEX 04 was designed to evaluate whether various populations and combinations of encoding schemes, probe templates, gallery templates, and fingerprint matchers will produce successful matches. In summary, the MINEX initiative was created to answer three main objectives: 1) Determine if standard templates give an accuracy comparable with proprietary (image-based) implementations. 2) Determine if template data can be generated and matched by different vendors without an attendant increase in error rates. 3) Establish compliance for template encoders and matchers for the United States Government's Personal Identity Verification (PIV) program.

Therefore, in this case the test was not designed to rank vendors but to determine whether various populations and combinations of encoding schemes, probe templates, gallery templates, and fingerprint matchers will produce successful matches. Each system participating was also required to produce minutiae templates in accordance with their proprietary encoding scheme. This provided a base performance level.

The experimental protocol, tests and results of MINEX 04 are thoroughly described in [NIST2006b]. Contrary to the two previous evaluation campaigns described in Sections 2.1 and 2.2, in this case the performance assessment was conducted for a verification scenario and not for identification. The results showed a clear performance loss between the three cases considered: 1) Proprietary template: vendor A performs recognition using its own proprietary templates. 2) Standard templates: vendor A performs recognition using its own extracted standard templates. 3) Interoperability: vendor A performs recognition using its matcher with the standard templates extracted by vendor B.

The results for the best performing system in the three scenarios are summarized in Table 3. In this case results are given in terms of the False Match Rate (FMR) and False Non-Match Rate (FNMR) which are accuracy metrics applied to the assessment of *verification* systems and not of AFIS. The two metrics may be defined as follows:

- False Match Rate (FMR): is the fraction of comparisons between samples of different individuals which are wrongly mated together.
- False Non-Match Rate (FNMR): is the fraction of comparisons between samples of the same individual which are wrongly non-mated.

	Proprietary template	Standard template	Interoperability
FNMR @ FMR=1%	0.47%	1.29%	3.08%

Table 3. Results of the best performing algorithm in MINEX 04 for the three considered scenarios. The figures represent the False Non-Match Rate (FNMR) at a False Match Rate (FMR) of 1%.

The MINEX program has its continuation with the MINEX-III test which pursues the same objectives as the original MINEX 04 evaluation. The algorithm submission period opened in June 2015.

The MINEX program was also extended in 2007 to the Match on Card technology with the MINEX-II initiative. The MINEX-II trials were conducted to evaluate the accuracy and speed of Match on Card verification algorithms that run on ISO/IEC 7816 smartcards. MINEX-II compared reference and verification data conforming to the ISO/IEC 19794-2 COMPACT CARD fingerprint minutia standard. The test was an assessment of the core viability of matching fingerprints (i.e. the de facto leading compact biometric data element) on personal identity credentials based on the industry-standard smart cards. The results are relevant to users of minutia templates as additional authentication factors and are collected in [NIST2011b]. This initiative is cited here for the sake of completeness, although it is less relevant to the SIS-II than the previous ones as the use of smart cards is not foreseen in the context of SIS-II.

2.5 Fingerprint Verification Competitions 2000, 2002, 2004, 2006 and OnGoing (FVC)

The series of Fingerprint Verification Competitions (FVC) organized by the Università di Bologna, started in the year 2000 as the first effort to independently evaluate, in a comparable framework, different fingerprint recognition systems. Before the FVC 2000 initiative, only a few benchmarks had been available for comparing developments in this area and developers usually performed internal tests in self-collected databases. Also, the lack of standards at that time had unavoidably led to the dissemination of confusing, incomparable and irreproducible results, sometimes embedded in research papers and sometimes enriching the commercial claims of marketing brochures.

The aim of the FVC initiative was to take the first steps towards the establishment of a common basis, both for academia and industry, to better understand the state-of-the-art and to have a clearer view as how to improve this technology in the future. The competitions were always presented as an effort to get a clearer picture of fingerprint technology capabilities in terms of accuracy but not as a performance certification of the systems due to the following points:

- The databases used in the contests were not acquired in a real environment.
- Only parts of the participants' software are evaluated by using images from sensors not native to each system. In fact, fingerprint-based biometric systems often implement proprietary solutions to improve robustness and accuracy (e.g. quality control modules to reject poor quality fingerprints, visual feedback to help the user in optimally positioning his/her finger, using multiple fingerprint samples to build more reliable templates, etc.) and these added-value modules were not taken into account in the competitions.

The experimental protocols and findings from these competitions are described in [Cappelli2006] and may be consulted at the BioLab webpage of the Università di Bologna13. A very brief summary of the results of the competitions is presented in Table 4 where the average performance of the best three algorithms for the different databases considered in the experiments is reported. It should be noticed that results are not comparable across competitions as the data used for each of them are not the same (i.e. four databases were used in all competitions, but always different). For instance, in FVC 2004 very bad quality samples were acquired on purpose (e.g. wet fingers, very dry skin, excessive pressure on the scanner, etc.) and were introduced into the tests to understand the impact of quality on the systems' performance.

Results in Table 4 are reported in terms of the Equal Error Rate (EER), which, for verification systems, is defined as the operating point where FMR=FNMR (see Section 2.4. for a definition of FMR and FNMR).

FVC2000	FVC2002	FVC2004	FVC2006	FVC-OnGoing
2.85%	0.29%	1.52%	1.97%	0.12%

Table 4. Average accuracy in terms of the Equal Error Rate (EER) of the best three performing algorithms over the different FVC databases. A direct comparison across different competitions is not possible due to the use of databases of unequal difficulty.

SECTION 2. SUMMARY OF KEY CONCEPTS:

- The **accuracy** of an AFIS is fully dependent on the **data** used for its evaluation, and more precisely on the **quality** of that data (see Section 3 for further details on biometric quality).
- Other factors that affect the performance of an AFIS are: size of the searched database, number of fingerprints used for the search, expected response time and size of the ranked list of identities returned by the system.
- Given good quality data and ten print *vs* ten print searches, independent evaluation campaigns have shown that the accuracy of current AFIS technology is very high, with error rates of around 0.1%.

[13] https://biolab.csr.unibo.it/home.asp

3 Fingerprint Quality

3.1 Introductory elements

As presented in Section 2, many studies and benchmarks have shown that the accuracy of biometric systems heavily depends on the quality of the acquired input samples [Alonso2012]. If quality can be improved, either by sensor design, user interface design or by standards compliance better accuracy will be obtained. For those aspects of quality that cannot be designed-in, an ability to analyse the quality of a live sample is needed. This is useful primarily in initiating the reacquisition from a user, but also for the real-time selection of the best sample, and the selective invocation of different processing methods. That is why quality measurement algorithms are increasingly deployed in operational biometric systems.

Biometric quality measurement has vital roles to play in improving biometric system accuracy and efficiency during the capture process (as a control-loop variable to initiate reacquisition), in database maintenance (sample update), in enterprise wide quality-assurance surveying, in invocation of quality-directed processing of samples and even in security-related tasks [Galbally2014]. Neglecting quality measurement will adversely impact the accuracy and efficiency of biometric recognition systems (e.g. verification and identification of individuals). Accordingly, biometric quality measurement algorithms are increasingly deployed in operational systems. These elements motivated the need for biometric quality standardization efforts.

This section, summarizes some of the main issues to be taken into account regarding the estimation of biometric quality and how it can be used to enhance the performance of biometric systems, giving an overall framework of the challenges involved. The section starts with some general concepts regarding biometric quality and then focuses on specific factors that concern fingerprint quality.

3.1.1 Signal quality and system accuracy

One of the main challenges faced by biometric technologies is accuracy degradation in less controlled environments such as, for instance, portable handheld devices or forensic scenarios (e.g. latent fingerprints). These environments will require robust recognition algorithms that can handle a range of changing characteristics. In such uncontrolled situations there are intrinsic operational factors that further degrade recognition performance and that are not generally replicated in controlled studies.

Conditions that are progressively more difficult significantly decrease performance, despite improvements in technology. In the 2000 and 2002 Fingerprint Verification Competitions (https://biolab.csr.unibo.it/fvcongoing), fingerprint data was acquired without any special restriction, resulting in a decrease of one order of magnitude in the Equal Error Rate. In 2004, researchers organising the competition intentionally corrupted samples (for example, by asking people to exaggeratedly rotate or press their finger against the sensor, or by artificially drying or moisturizing the skin with water or alcohol). Logically, a corresponding performance decrease occurred.

3.1.2 What is biometric sample quality?

Broadly, a biometric sample is of good quality if it is suitable for personal recognition. Recent standardization efforts (ISO/IEC 29794-1) have established three components of biometric-sample quality:

- *Character* indicates the source's inherent discriminative capability.
- *Fidelity* is the degree of similarity between the sample and its source, attributable to each step through which the sample is processed.
- *Utility* is a sample's impact on the biometric system's overall performance, where the concept of sample quality is a scalar quantity that is related monotonically to the performance of the system.

3.1.3 What is a biometric quality metric?

Essentially, a quality metric is a function or algorithm that takes as input a biometric sample and outputs a value or score defining the quality of the sample. It is important to note that automatic quality metrics do not necessarily measure quality in the same way that humans perceive it, therefore, their results are not always aligned with the subjective quality estimation of experts [Langenburg2012].

Researchers have developed quality assessment algorithms mainly for fingerprint, iris, voice, face, and signature. Unfortunately, almost all of the many algorithms have been tested under limited, heterogeneous frameworks. This diversity of test conditions is due primarily to the fact that the biometrics community has only recently formalized the concept of sample quality and developed evaluation methodologies.

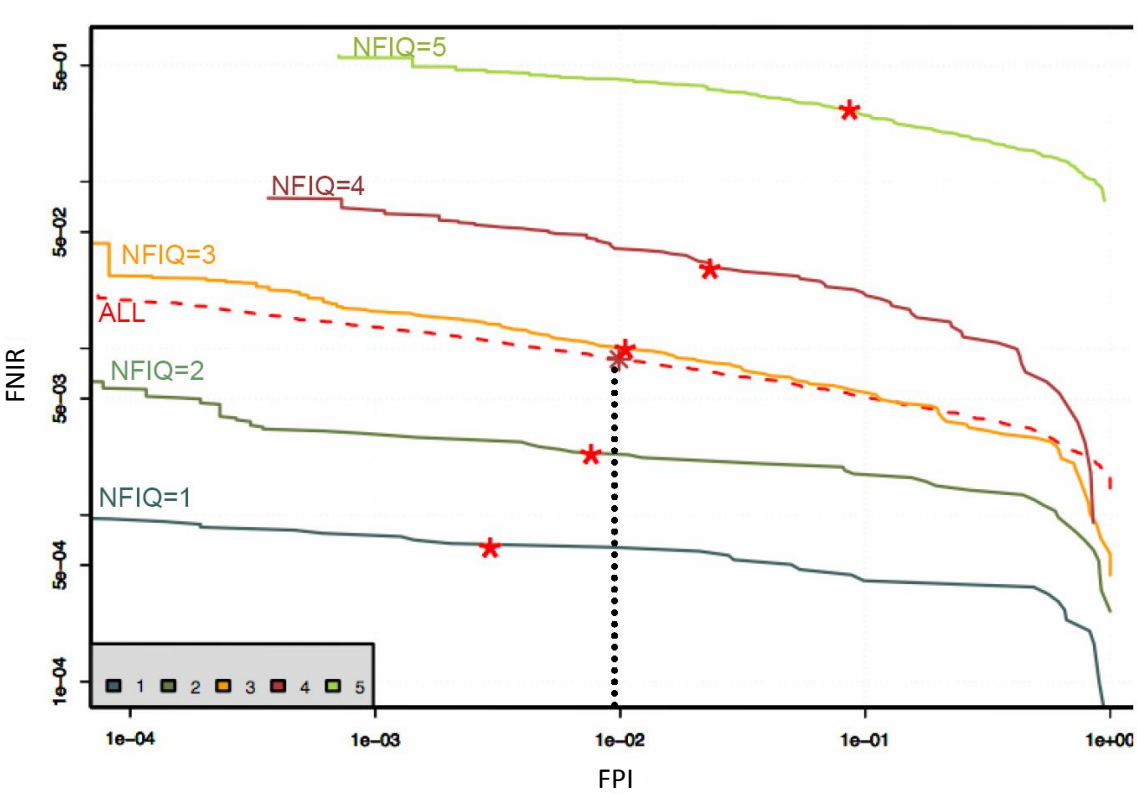

Figure 1. DET curves (see Annex 1 for further details on this accuracy metric) corresponding to the same fingerprint recognition system working on different quality fingerprint groups. It can be observed that, as the quality of the data used is higher (from 5 to 1) the accuracy of the system significantly improves. The figure has been extracted from [Tabassi2007]

One of the biggest challenges to be faced by biometric quality metrics is the fact that although biometric matching involves at least two samples, these are not acquired at the same time. Reference samples are stored in the system database and are later compared with new samples provided during system operation. So, a quality assessment algorithm should be able to work with individual samples, even though it ultimately aims to improve recognition performance when matching two or more samples.

One of the main characteristics a quality metric is expected to present is to mirror the sample's *utility* so that higher-quality samples lead to better identification of individuals. Accordingly, quality should be predictive of recognition accuracy. This concept was formalized in [Grother2007], where the authors presented a framework for evaluating and comparing quality measures in terms of the capability of predicting system performance. Broadly, they defined biometric sample quality as a scalar quantity monotonically related to the biometric matchers' recognition accuracy when that

biometric sample is used for recognition. By partitioning the biometric data into different groups according to certain quality criteria, the quality measure will give an ordered indication of accuracy between quality groups. This effect is shown in Figure 1 which depicts the DET curves (see Annex 1 for a definition of DET curves) for different fingerprint quality groups annotated using NFIQ (further details about NFIQ are given in Section 3.4.). It can be observed that the best accuracy of the system is obtained for the data of the best quality group (i.e. NFIQ=1) and then gradually deteriorates for the rest of the groups. This way, the rejection of low-quality samples will decrease error rates in proportion to the fraction rejected.

3.2 Factors affecting fingerprint quality

Quality factors may be classified on the basis of their relationship with the system's different parts. We propose to distinguish five classes:

- Origin-related,
- User-related,
- User-sensor interaction,
- Acquisition sensor,
- Processing-system factors.

Each of these factors is briefly analysed in the following sections.

3.2.1 Origin-related factors: live-scanned, inked and latents

In the case of AFIS used for law-enforcement purposes, such as potentially the SIS-II system, the feature extraction and matching algorithms have to cope with samples produced from multiple sources which can present very different quality levels. In particular:

- *Live-scanned fingerprints*: this is nowadays the most extended form of fingerprint acquisition device. Samples acquisition uses sensors that directly produce a digital image of the fingerprint. Although most usual scanners are based on optical technology, other solutions are also available on the market such as capacitive or ultrasound sensors. In general, optical scanners produce the best quality.
- *Inked fingerprints*: this corresponds to the traditional way of fingerprint acquisition. In this case the person whose fingerprint is being acquired places his/her finger on an ink pad and then immediately onto paper. The whole process is guided and supervised by a human operator. Then, the fingerprint image is digitalized with a scanner. Although such an acquisition method is becoming obsolete there is still a non-negligible percentage of fingerprints that are acquired using this procedure. Furthermore, the vast majority of fingerprints dating from more than 15-20 years ago, before the arrival of the new live-scanning technology, are inked samples, especially in the law enforcement domain. Therefore, current fingerprint recognition systems and especially those intended for law enforcement use, are required to be compatible with this type of sample.
- *Latent fingerprints*: contrary to the previous two categories, in this case the person whose fingerprints are being processed is not present at the moment of the acquisition. The fingerprints are lifted from a surface touched by the individual and digitalized in successive steps. In general, latent fingerprints are only relevant in the framework of law-enforcement contexts such as SIS-II. Regarding quality, latent fingerprints pose a huge challenge as there is no possibility to reacquire the sample. Furthermore, as there is obviously no user cooperation, latents in general present low quality features including: limited availability of ridge patterns, brush strokes, circular markings, background noise, stains etc. [Yoon2013].

Further discussion on the different type of fingerprint data that AFIS have to deal with may be found in Annex 1.

3.2.2 User-related factors

These factors include physical/physiological and behavioural factors. As they are entirely related to the user — a person's inherent features are difficult or impossible to modify — they are the most difficult to control.

Physical/physiological. These include, for instance, age or gender — subjects cannot alter these features depending on the biometric system being used. Therefore, recognition algorithms must account for data variability in these categories. Also, diseases or injuries can alter features such as the finger, sometimes irreversibly, possibly making them impractical for recognition.

- The user's *age* can affect recognition in several ways. Although fingerprint characteristics are highly stable, they change until adolescence and during old age [JRC2013].
- *Gender* can cause differences as female fingerprints tend to present narrower ridges which are closer together.

Behavioural. Sometimes, people can modify their behaviours or habits. It is possible to alleviate many behavioural factors by taking corrective actions. However, this is not always possible, such as in forensic or surveillance applications. On the other hand, depending on the application, such corrective actions could be counterproductive, resulting in subjects being reluctant to use the system. In general, the supervision of the acquisition process by a well-trained human operator can reduce, to a large extent, the influence of these factors. Some of these factors include:

- Tiredness, distraction, cooperativity, motivation, nervousness.
- Pressure against the sensor.
- Inconsistent contact.
- Skin condition, which refers to factors such as skin moisture, sweat, cuts and bruises.
- Manual labour might affect the skin condition, in some cases irreversibly.

3.2.3 User-sensor interaction factors

In principle, these factors, which include environmental and operational factors, are easier to control than user-related factors, provided that it can be possible to supervise the interaction between the user and the sensor — for example, in controllable premises such as a police station. As in the previous case, the supervision of the acquisition process by a well-trained human operator can reduce, to a large extent, the influence of the following parameters:

- *Outdoor operation* is especially problematic because control of other environmental factors can be lost. It also demands additional actions regarding sensor condition and maintenance.
- *Temperature* and *humidity* affect skin properties (in fingerprint and palm print recognition).
- *Feedback* to the user regarding the acquired data has been demonstrated to lead to better acquired samples, which can lead to *user familiarity* with the system.

3.2.4 Acquisition sensor factors

As mentioned previously, a growing majority of current fingerprints are acquired using specific live-scanned sensors. In this case, the sensor is the only physical point of interaction between the user and the fingerprint system. Therefore, its fidelity in reproducing the original fingerprint pattern is crucial for the recognition system's accuracy. The diffusion of low-cost sensors and portable devices is rapidly growing in the context of widening access to information and services. This represents a new scenario for automatic fingerprint recognition systems.

Unfortunately, these low-cost, portable devices produce data very different from that obtained by dedicated, more expensive sensors. This is primarily due to smaller input areas, poor ergonomics, and the possibility of user mobility. Additional problems arise when data from different devices coexist in a fingerprint system—something common in multi-vendor markets. Algorithms must account for data variability in this scenario of sensor interoperability — something that can be achieved through the use of the following quality measures:

- *Time between acquisitions* can greatly affect system performance because data acquired from an individual at two different moments might differ considerably.
- Sensors sometimes incorporate *physical guides* to facilitate acquisition (for example, for fingerprint and palm print recognition).
- *Ergonomics* refers to how the acquisition device's design facilitates user interaction.

3.2.5 Processing-system Factors

These factors relate to how a biometric sample is processed after it has been acquired. In principle, they are the easiest to control. Constraints on storage or exchange speed might impose data compression techniques — for example in the case of smart cards. Also, governments, regulatory bodies or international standards organizations might specify that biometric data must be kept in raw form (rather than in post-processed templates that might depend on proprietary algorithms), which could affect data size.

3.3 Incorporating quality in fingerprint recognition systems

Quality measurement algorithms can be used to modify and improve the processing and final performance of biometric systems. Such influence in the general working flow of the system includes:

Quality-based processing. An identification system might apply image restoration algorithms or invoke different feature extraction algorithms for samples with some discernible quality problem.

- Quality-specific enhancement algorithms.
- Conditional execution of processing chains, including specialized processing for poor-quality data.
- Extraction of features robust to the signal's degradation.
- Extraction of features from useful regions only.
- Ranking of extracted features based on the local regions' quality.

Template updating (updating of the enrolment data and database maintenance). A quality measurement may be used to determine whether a newly-acquired sample should replace the already enrolled sample. Some systems combine old and new sample features. Quality can be used in both processes.

- Storing multiple samples representing the variability associated with the user (for example, different portions of the fingerprint to deal with partially overlapped fingerprints).
- Updating the stored samples with better-quality samples captured during system operation.

Quality-based matching, decision, and fusion. Certain systems may invoke a slower but more powerful matching algorithm when low-quality samples are compared. Also, the logic that provides acceptance or rejection decisions may depend on the measured quality of the original samples. This might involve changing a verification system's operating threshold for poor quality samples. For example, in multimodal biometrics, the relative qualities of samples of the separate modes may be used to augment a fusion process by:

- Using different matching or fusion algorithms,
- Adjusting those algorithms' sensitivity,
- Quantitative indication of acceptance or rejection reliability,
- Quality-driven selection of data sources to be used for matching or fusion — for example, weighting schemes for quality-based ranked features or data sources.

Monitoring and reporting across the different parts of the system help to identify problems leading to poor-quality signals and initiate corrective actions. This process can assess signal quality according to these factors:

- *Application*. Different applications might require different scanners, environment set-ups, and so on, which might have different effects on the acquired signals' overall quality.
- *Site or terminal*. Such assessment identifies sites or terminals that are abnormal owing to operator training, operational and environmental conditions etc.
- *Capture device*. Such assessment identifies the impact due to different acquisition principles, mechanical designs etc. It also determines whether a specific scanner must be substituted if it doesn't provide signals that satisfy the quality criteria.
- *Subject*. Such assessment identifies interaction learning curves, which can help better train new users and alleviate the "first-time user" syndrome.
- *Stored template*. Such assessment detects how the database's quality varies when new templates are stored or old ones are updated.
- *Biometric input*. If the system uses multiple biometric traits, such assessment improves how they're combined.

Monitoring and reporting can also support trend analysis by providing statistics from all applications, sites etc. This will let analysts identify trends in signal quality or sudden changes that need further investigation.

3.4 NFIQ and NFIQ-II

As mentioned previously in this document, a number of factors can affect the quality of fingerprint images: occupation, motivation/collaboration of users, age, temporary or permanent cuts, dryness/wetness conditions, temperature, dirt, residual prints on the sensor surface, etc. Unfortunately, many of these factors cannot be controlled and/or avoided. For this reason, assessing the quality of captured fingerprints is important for a fingerprint recognition system.

Fingerprint quality is usually defined as a measure of the clarity of ridges and valleys and the extractability of the features used for identification such as minutiae, core and delta points etc. In other words, most of the operational schemes for fingerprint image-quality estimation are focused on the *utility* of the images, that is, their correlation to system performance.

This relationship between a quality metric and biometric recognition performance however, is largely subjective: not all recognition algorithms work the same way (that is, they are not based on the same features), and their performance is not affected by the same factors. For example, fingerprint recognition algorithm A might be insensitive to rotation changes, whereas such changes severely affect algorithm B. In this situation, a measure of rotation will be useful for predicting B's performance but not A's. Therefore, an algorithm's efficiency will usually be linked to a particular recognition algorithm or class.

For the above reason, many different quality approaches, both local and global, have been proposed in the literature [Alonso2010]. However, in spite of all the efforts dedicated to the estimation of fingerprint quality, there is still no standard method which has been proven to outperform the rest for all possible recognition contexts (e.g. type of matcher, type of fingerprint, sensors).

Such a lack of a unified way of measuring fingerprint quality drove the American National Institute for Standards and Technology (NIST) to develop, in 2004, the NIST Fingerprint Image Quality (NFIQ) algorithm as part of their public software package NIST Biometric Image Software (NBIS). Since then, the NFIQ has become the *de facto* standard for fingerprint quality estimation and a second improved version of the algorithm, the NFIQ-II, is currently being developed and is expected to be released in September 2015. Further details regarding NFIQ and NFIQ-II are given below:

- **NFIQ**. In 2004 NIST released the NIST Fingerprint Image Quality algorithm (NFIQ). Its key innovation with regard to previously-proposed fingerprint quality algorithms is to produce a quality value from a fingerprint image that is directly predictive of expected matching performance. The algorithm has shown very consistent performance regarding quality estimation over very different set-ups and is now being used in many practical applications as

a reliable metric. As such, it is also cited in most fingerprint quality-related publications to give baseline results with which to compare those of novel methods. In addition its computation is mandatory in the ANSI/NIST ITL 1-2007 standard (see Section 0).
The algorithm, fully described in [NIST2004b], is based on a number of known fingerprint quality features which are given as input to a neural network previously trained on tagged data. The algorithm takes as input images that are in different format such as ANSI/NIST or NIST IHEAD or compressed using WSQ, baseline JPEG or lossless JPEG. The quality features are extracted from the image and given as input to the neural network which assigns to each input fingerprint image one of five quality levels (one being the highest quality and five being the lowest). As mentioned before, the source code for the algorithm is freely available as part of the NBIS distribution which is perhaps one of the most important reasons for its wide adoption. While the NFIQ algorithm provides a very good open-source means for determining fingerprint quality, its capability for determining accuracy of a specific AFIS algorithm will, in principle, be lower than a vendor-specific quality algorithm.

- **NFIQ-II**. With advances in fingerprint technology since 2004, an update to the NFIQ algorithm was proposed by NIST. A workshop was held in March 2010 at NIST to address the technical status of fingerprint quality assessment technology and to engage industry to improve core finger image quality assessment technology based on lessons learned from recent deployments of quality assessment algorithms (including NFIQ) in large-scale identity management applications. Led by NIST and by Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany, a team of biometric experts, from researchers to developers and vendors, was set up in order to give the members' input for the development of NFIQ-II. The release of the final publicly-available software tool is foreseen for September 2015 with multiple improved features with respect to the first version of NFIQ; among them: an improved quality feature set, a higher number of quality levels (from five to 100), faster and lighter implementation, better performance and a modular design that allows for self-training the neural network classifier on various categories of data. Another determinant added value is that this second version of the software will be open source. As such, it will allow users to better integrate it within their systems. The original distribution of the package will be released with an optimized solution to estimate the quality of 500dpi live-scanned fingerprints coming from adults and captured with optical scanners. However, its open source dimension and its modular design will permit re-training of the system in order to optimize it to the quality of other type of fingerprint data (e.g. latents, children's fingerprints, inked samples etc.)

3.5 Standards for biometric quality

Biometric data interchange standards are needed to allow the recipient of a data record to successfully process data from an arbitrary producer. In other words, biometric interoperability and the phrase ''successfully process the data" mean that the Biometric Sample Quality score can be accurately exchanged and interpreted by different applications. This can only be achieved if the data record is both syntactically and semantically in compliance with the documentary standard.

Following advances in biometric technologies as a reliable identity authentication technique, more large-scale deployments (e.g. e-passport) involving multiple organizations and suppliers are being rolled out. Therefore, in response to a need for interoperability, biometric standards have been developed.

Without interoperable biometric data standards exchange of biometric data among different applications is not possible. Seamless data sharing is essential to identity management applications when enrolment, capture, searching and screening are done by different agencies, at different times, using different equipment in different environments and/or locations. Interoperability allows modular integration of products without compromising architectural scope, and facilitates the upgrade process and thereby mitigates risk of obsolescence.

This section focuses on biometric quality standardization. Broadly, biometric quality standards serve the same purpose as many other standards, which is to establish an interoperable definition, interpretation and exchange of biometric quality data. Like other standards, biometric quality standards create grounds for a marketplace of off-the-shelf products and are also a necessary condition in order to achieve supplier independence and to avoid vendor lock-in.

Table 5 below lists the main standards organizations and other bodies working on the development of biometric standards. Current development focuses on acquisition practices, sensor specifications, data formats and technical interfaces. Also, a registry of US-government-recommended biometric standards (www.biometrics.gov/standards) offers high-level guidance for their implementation. The two main entities working in biometrics standards are the ISO/IEC JTC 1/SC 37 and the ANSI/NIST.

Concerning the specific incorporation of quality information the two most relevant efforts are:

- The ISO/IEC 29794 Biometric Sample Quality Standard.
- The ANSI/NIST ITL 1-2007 Quality Field.

Biometric standard organizations
International Standards Organizations: - IEC: International Electrotechnical Commission (www.iec.ch) - ISO-JTC1/SC37: International Organization for Standardization, Committee 1 on Information Technology, Subcommittee 37 for Biometrics (www.iso.org/iso/jtc1_sc37_home)
National standards bodies: - ANSI: American National Standards Institute (www.ansi.org)
Standards-developing organizations: - ICAO: International Civil Aviation Organization (www.icao.int) - INCITS M1: International Committee for Information Technology Standards, Technical Committee M1 on Biometrics (http://standards.incits.org/a/public/group/m1) - NIST-ITL: American National Institute of Standards and Technology, Information Technology Laboratory (www.nist.gov/itl)
Other organizations: - BC: Biometric Consortium (www.biometrics.org) - BCOE: Biometric Center of Excellence (www.biometriccoe.gov) - BIMA: Biometrics Identity Management Agency (www.biometrics.dod.mil) - IBG: International Biometric Group (www.ibgweb.com) - IBIA: International Biometrics and Identification Association (www.ibia.org)

Table 5. Main organizations working on the development of Biometric standards

3.5.1 The ISO/IEC 29794 Biometric Sample Quality Standard

The SC37 Biometrics Subcommittee of JTC1 has published the ISO/IEC 29794, a multi-part standard that establishes quality requirements for generic aspects (Part 1), fingerprint image (Part 4), facial image (Part 5) and, possibly, other biometrics at a later stage. Specifically, part 1 of this multi-part standard specifies derivation, expression and interpretation of biometric quality, regardless of modality. It also addresses the interchange of biometric quality data via the multi-part ISO/IEC 19794 Biometric Data Interchange Format Standard. Part 4 addresses the aspects of biometric sample quality that are specific to finger images ISO/IEC 19794-4.

The generic ISO/IEC 29794-1 requires that quality values must be indicative of recognition performance in terms of false match rate, false non-match rate, failure to enrol and failure to acquire. This part defines a binary record structure for the storage of a sample's quality data. It establishes requirements on the syntax and semantic content of the structure. Specifically, it states that the purpose of assigning a quality score to a biometric sample shall be to indicate the expected utility of

that sample in an automated comparison environment. That is, a quality algorithm should produce quality scores which target application specific performance variables.

3.5.2 The ANSI/NIST ITL 1-2007 Quality Field

Initiated in 1986, this standard is the earliest and most widely deployed biometric standard. It establishes formats for the mark-up and transmission of textual, minutia and image data between law enforcement agencies, both within United States and internationally.

The ANSI/NIST standard includes defined Types for the major biometric modalities. The standard is multimodal in that it allows a user to define a transaction that would require, for example, fingerprint data as Type 14, a facial mugshot as Type 10 and the mandatory header and metadata records Type 1 and 2. These are linked with a common numeric identifier.

In its latest revision, it allows for multiple quality fields where each quality score could be computed by a different quality algorithm supplier. In addition, it mandates NIST Fingerprint Image Quality (NFIQ) for all Type 14 records.

SECTION 3. SUMMARY OF KEY CONCEPTS:

- The **performance** of an AFIS is fully dependent on the **quality** of the data (i.e. fingerprint samples) it runs on.
- Many factors can affect the quality of fingerprints. Some of these factors are controllable (i.e. cleanliness of the sensor) and others are not (i.e. eroded fingerprints due to manual work).
- Automatic **fingerprint quality metrics** play an essential role in the control of the quality of the data enrolled to an AFIS.
- Different types of fingerprints can present very different quality levels. The main type of fingerprints an AFIS has to deal with are: inked/live-scanned, rolled/flat/latents.
- The most challenging data in terms of performance for an AFIS are **latents** because there is no control over their quality (which is usually very poor).
- Although there is no unique standard way of measuring fingerprint quality, NFIQ and NFIQ-II have become *de facto* standards thanks to their proven very high performance and availability.
- Multiple quality scores can be included for the same ten prints card.

4 Member States National AFIS: Common Technical Usage and Operational Diversity

The end-users of a future AFIS functionality introduced in SIS-II will be the law enforcement and border authorities of the different Member States (MS). As such, during the design process of such an AFIS, it can be very instructive to have detailed information on the national AFIS already being used in order to learn from the expertise already acquired and the best practice developed.

With this purpose, the present section summarizes all the relevant features gathered during the visits and discussions that the JRC conducted in nine Member States' national AFIS (see Section 1.3.2). The section is divided into three main parts:

- a first subsection describing the technical use-cases given to AFIS technology in the different MS,
- a second subsection which accounts for the differences observed in the operational use of AFIS technology,
- a last subsection where some indicative figures regarding the size of the different national AFIS are given,

It is important to underline that the objective of this section is not to present an exhaustive categorization of the national AFIS features on a country by country basis, but rather to highlight from a general point of view the main common points and differences observed in our visits. We believe that such a summary can help to obtain a clearer picture of the uses and operational specificities of current AFIS technology and facilitate their application to SIS-II.

Different terms such as ten print matching, hit/no-hit, latent fingerprints or ranked list of identities are used throughout the section. These concepts are defined in Annex 1.

4.1 Common technical use cases processed by National AFIS

From a generic technical perspective as well as from the implementations pointed out by the different law-enforcement entities visited in the course of the study, use-cases may be listed in five main groups (detailed below), according to:

- Origin of the fingerprints used for the consultation of the database. They may come from:
  - A person who is (or was) present at the time of the fingerprint acquisition (e.g. a suspect who has been arrested);
  - Latent fingerprints lifted at a crime scene.
- Origin of the fingerprints stored in the database against which the query is performed. The same two possibilities apply as before.

For each of the five main technical use-cases defined below, two basic parameters need to be defined, namely:

- Minimum expected accuracy of the matching process.
- Maximum permitted response time.

In the short descriptions of the five technical use-cases given below, some figures are given for each of these two parameters (i.e. accuracy and response time). The values are presented solely for illustrative purposes, they are the result of the previous consultations of the SISVIS committee, the visits undertaken by the JRC and the scientific literature. However, they can help to understand the

differences among use-cases and the various requirements that have to be met in each of the possible scenarios.

For all the use-cases and examples given in this section, ten print cards are assumed to contain both flat and rolled fingerprint samples. For a more precise definition of the different types of fingerprint data commonly used (e.g. flat/rolled, inked/live-scanned, latents, etc.) see Annex 1.

As a visual aid to understand the differences among the five considered technical use-cases, a schematic flow chart is given for each use-case (Figure 2 to Figure 6).

4.1.1 TECHNICAL USE-CASE 1: ten print vs ten print

- Origin query fingerprints: a person who is present at the time of the fingerprint acquisition (ten print card).
- Origin searched database: a person who is (or was) present at the time of the fingerprint acquisition (ten print card)

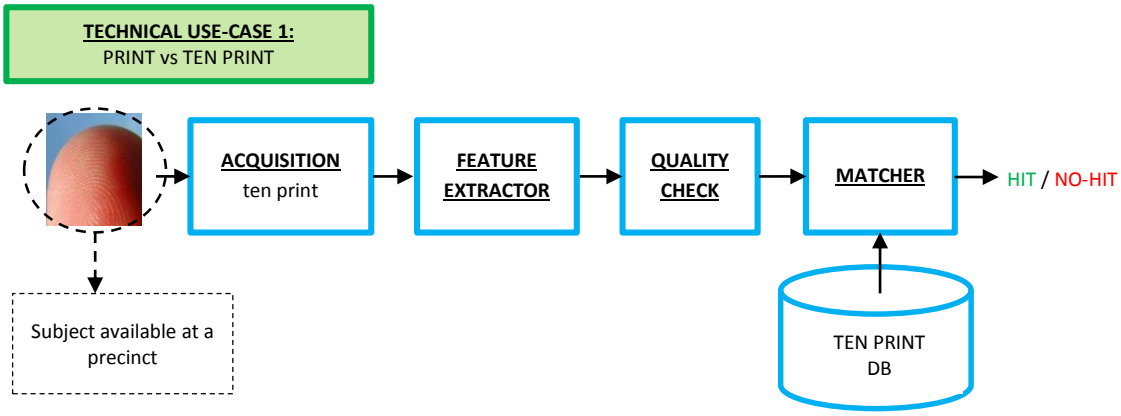

Figure 2. Flow-chart corresponding to the technical use-case 1 (i.e. ten print vs ten print) identified in the visits to the national AFIS

The typical situation illustrated in Figure 2 would be as follows: a person is arrested, taken to a police station and his/her ten print card is acquired. The ten print card is used to search in the central ten print database. Therefore, in this case the searched person is present both at the time of the acquisition of his/her ten print data and at the time the query is sent to the system (both actions are conducted within the same short frame of time).

A possible variant of this scenario is that some pre-existing ten print data is used to carry out a query against the central ten print database. That is, the searched person was arrested some time ago in one of the Member States. As such, the person was present when his/her ten print data was acquired, but he/she is no longer be present when the actual search is conducted.

In this use-case both the query ten print data and the ten print data stored in the database are acquired under strong supervision and by applying best-practice techniques, therefore, a very high quality can be expected. As such, the requirement for the expected accuracy of the system can be set very high.

On the other hand, the suspect has been arrested and taken to a police station for some motive, therefore, the suspect can be held in custody for some period of time (usually several hours). As such, the response time of the system is not the most critical factor.

- Minimum expected accuracy (hit – no hit, i.e. ranked list of size 1): higher than 99.9%
- Maximum permitted response time (this is not a critical requirement): up to ten minutes

4.1.2 TECHNICAL USE-CASE 2: Two print flat vs ten prints (fast identification)

- Origin query fingerprints: a person who is present at the time of the fingerprint acquisition (2 live-scanned fingerprints flat).
- Origin searched database: a person who was present at the time of the fingerprint acquisition (ten print card)

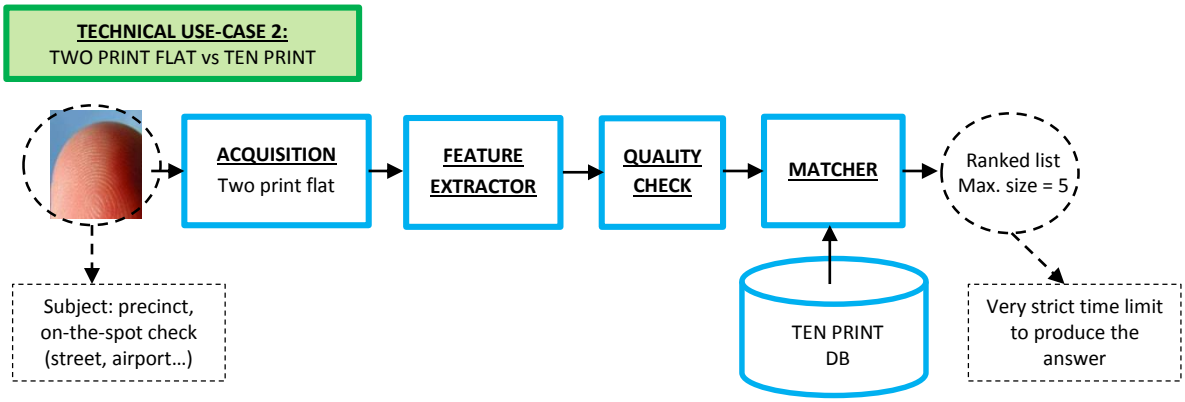

Figure 3. Flow-chart corresponding to the technical use-case 2 (i.e. fast identification or two print vs ten print) identified in the visits to the national AFIS

The typical scenario illustrated by Figure 3 for this use-case would be as follows: a person is stopped (not necessarily arrested) to perform some check and two fingerprints are acquired with a live-scan flat sensor. Those two fingerprints are used to carry out a fast search in the ten print database.

This use-case case could be helpful to perform on-the-spot checks in case a suspicion arises or in the frame of checks of a large population in a limited period of time (e.g. border checks at airports or checks in the street).

Since the query data are two flat fingerprints (and not a ten print card as in the technical use case 1) the expected accuracy cannot be as high as in the previous case. However, there is still full control over the acquisition process both of the query and the searched data. For these reasons the accuracy can still be high over a short ranked list of candidates. In case the searched person is present in that list, he/she can be sent to a second line check where technical use-case 1 may be used.

In this case the searched person does not necessarily need to be arrested, he/she cannot be detained for long. Accordingly, the response time becomes a critical parameter for this particular use-case as the whole process (i.e. fingerprint acquisition and query) must be kept as fast as possible.

- Minimum expected accuracy (ranked list of five): higher than 99.9%.
- Maximum permitted response time: 20 to 30 seconds.

4.1.3 TECHNICAL USE-CASE 3: Latent vs ten print

- Origin query fingerprints: latent fingerprints lifted at crime scenes
- Origin searched database: a person who is (or was) present at the time of the fingerprint acquisition (ten print card).

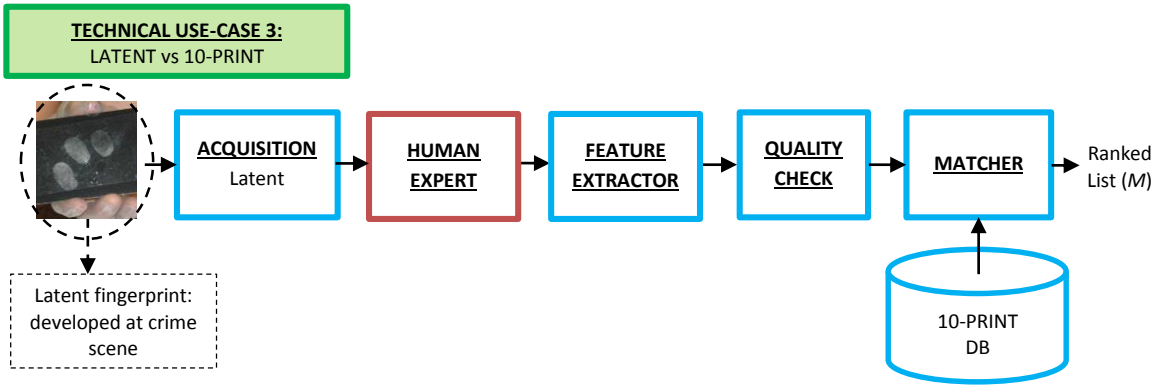

Figure 4. Flow-chart corresponding to the technical use-case 3 (i.e. latent vs ten print) identified in the visits to the national AFIS

The typical scenario illustrated in Figure 4 for this use case would be as follows: a latent fingerprint is found at a crime scene. It is used to launch a query against the central ten print database.

This use-case represents a current real challenge for AFIS in terms of accuracy as there is no supervision or control at the time when the fingerprint was left behind. This means that the quality of the latent used as query data can be anywhere from very high to very poor. For this reason the intervention of human experts is, in principle, mandatory during the encoding process of the latent prior to the search in the database. Even so, it is not possible to set a strict limit on the accuracy or on the size *M* of the ranked list (this will be very dependable on the quality of the latent, the importance of the case etc.)

Regarding the maximum response time, it is in principle not a critical parameter as there is no person being retained. However some Member States are working on a faster latent procedure applied only for narrowing an ongoing investigation in the frame of a terrorism crime for which response time can become critical. Any value from few to several minutes can be acceptable in most of the cases.

- Minimum expected accuracy (ranked list of *M*): as high as possible (it depends on the query data, need for a performance evaluation campaign with **real** data).
- Maximum permitted response time (this is not a critical requirement): 20 to 120 minutes.

4.1.4 TECHNICAL USE-CASE 4: ten print vs latent

- Origin query fingerprints: a person who is (or was) present at the time of the fingerprint acquisition (ten print card).
- Origin searched database: latent fingerprints lifted at crime scenes and stored in database as unsolved cases

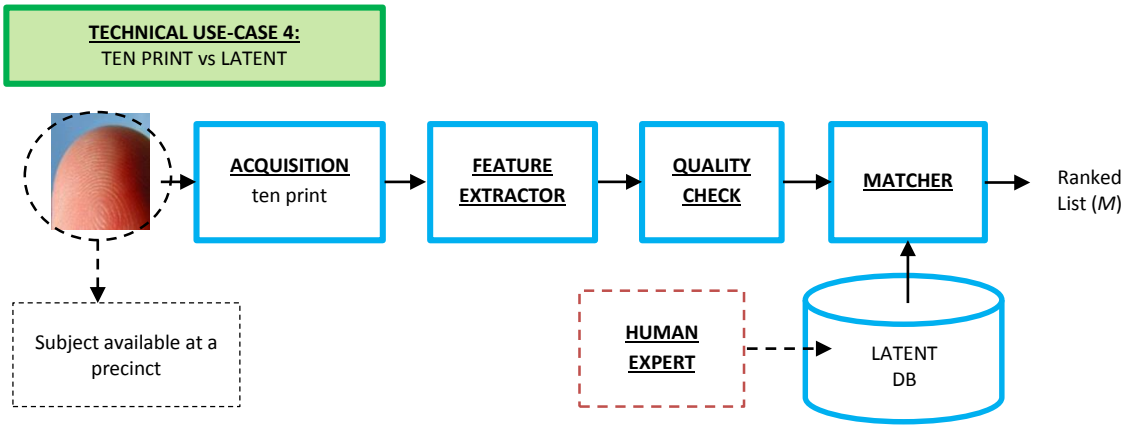

Figure 5. Flow-chart corresponding to the technical use-case 4 (i.e. ten print vs latent) identified in the visits to the national AFIS

The typical scenario illustrated in Figure 5 for this use case would be as follows: a person is arrested. The person is searched in the database of ten print known identities (technical use case 1). Independently of whether he/she is identified or not, he/she is also searched in a database of latent fingerprints to determine if she/he might be linked with previous crimes where the author was never captured but the found latent stored in the database.

This case is similar to that described in technical use-case 1 (i.e. ten print vs ten print). The main difference is that the searched database comprises latent fingerprints as well. As such, some human intervention in the processing of the latents is required before storing them in the database.

As in technical use-case 3, in the present scenario the identification task involves latent fingerprints. Consequently it is not possible to set a requirement for the minimum accuracy of the system as this will be very dependent on the quality of the latent samples stored in the database. The final size (*M*) of the candidate list will depend on the expected accuracy of the system on the given database (for a lower accuracy a larger *M* will be needed, while a higher accuracy allows for a smaller *M*).

Similar to technical use-case 1, the response time is not critical since, typically, the arrested person can be held for up to several hours depending of the Member States specific legislation and the reasons for the arrest.

- Minimum expected accuracy (ranked list of *M*): as high as possible (it depends on the searched data, need for a performance evaluation campaign with **real** data).
- Maximum permitted response time (this is not a critical requirement): up to 120 minutes.

4.1.5 TECHNICAL USE-CASE 5: latent vs latent

- Origin query fingerprints: latent fingerprint lifted at crime scene
- Origin searched database: latent fingerprints lifted at crime scenes and stored in database as unsolved cases

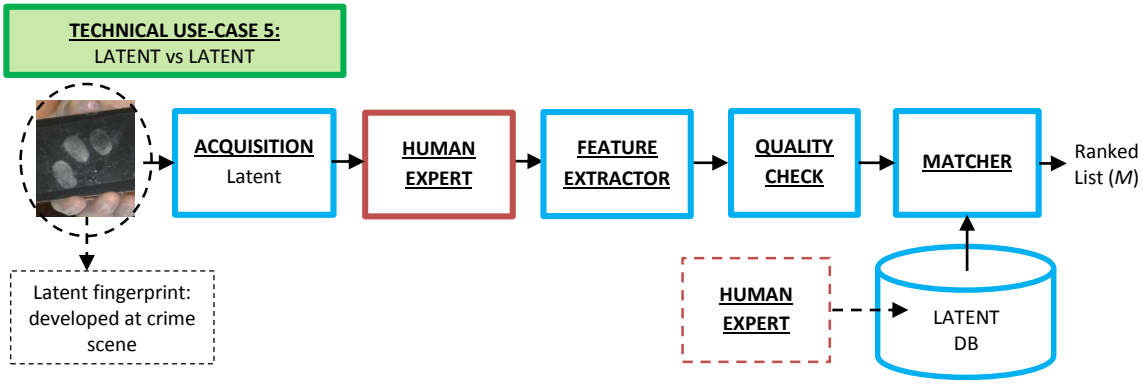

Figure 6. Flow-chart corresponding to the technical use case 1 (i.e. latent vs latent) identified in the visits to the national AFIS

The typical scenario illustrated in Figure 6 for this use case would be as follows: a latent fingerprint is found at a crime scene. It is searched in the ten print database of known identities (technical use-case 3). Independently of whether it is identified or not, it is also searched in the database of latent fingerprints to determine if the same person committed some previous crime for which he was not arrested.

This is probably the most challenging use-case from a technical perspective as there is no control on the quality of either the query or the searched data. Consequently, this is the use-case where the lowest performance of the AFIS may be expected and therefore where the largest size *M* of the final ranked list is required. It should also be highlighted that this is a much rarer use-case than all previous examples.

The response time requirements for this case are even more flexible than in the technical use-case 4 as this scenario does not involve the arrest of a suspect.

- Minimum expected accuracy (ranked list of *M*): as high as possible (it depends on the searched data, need for a performance evaluation campaign with **real** data).
- Maximum permitted response time (this is not a critical requirement): up to 120 minutes.

4.2 Further technical diversity of implemented national AFIS

In addition to the five common use-cases identified in all the deployed national AFIS described in the previous section, further operational differences have been found in the different national AFIS visited (see Section 1.3.2.) which are reported in this section. In general, these differences mainly affect the methodologies followed in the operational procedures of the AFIS, which may vary from country to country.

Acquisition technology. For the acquisition process, although live-scan sensors are currently a growing solution and the only option selected for new deployments, the traditional paper-and-ink method is still used in numerous cases.

Fingerprint image resolution. The worldwide de facto standard for the resolution of fingerprint images is 500dpi. As such, the current live-scanners used at the visited MSs acquire 500dpi images. It is true that there is a recent and growing trend in the production of 1000dpi sensors which require a higher storage capacity and processing power as the produced images are significantly larger than those produced by standard 500dpi scanners. Some of the AFIS in the MS are compatible with this

type of higher resolution image. However, even though some of the visited AFIS are able to store and process 1000dpi images, these samples are down-scaled to 500dpi prior to performing automatic matching. Therefore, for the moment, 1000dpi images are basically used solely for visualization purposes (by human examiners) but the actual automatic identification uses the current standard of 500dpi. In fact, different works have analysed the impact of image resolution on the final accuracy of AFIS and have not found any significant difference between 500dpi and 1000dpi images. Even so, the growing use of 1000dpi sensors should be taken into account in the implementation of new AFIS.

Human intervention. Some Member States decided to completely rely on the automatic capabilities of their national AFIS to encode the fingerprint templates without human expert intervention. Those system or at least the parts of those system which are fully automatic are also called "lights out" systems. Other Member States complement the fully automatic coding of templates with the systematic intervention of fingerprint experts in order to validate the coding and to improve, when necessary, the positioning of the fingerprint minutiae not only in the case of latent fingerprints (which is the case for all of them) but also for ten prints cards. In all cases an automatic quality check is performed at the time of acquisition. If the quality is not good enough, the fingerprint is reacquired until it passes the threshold. If the minimum quality threshold is still not reached, the fingerprint is processed by a human expert who detects, possibly complements and validates the minutiae points. The main trend observed is that as the system improves from a quality and accuracy points of view, the rôle of human intervention tends to decrease accordingly. Still this human intervention remains a key factor for accuracy in numerous scenarios and the promotion of best practice will further support the increase of accuracy in an AFIS.

Fast consultations. As described in Technical Use-Case 2, some Member States have developed fast consultation of their national AFIS. These consultations can be performed with ten prints flat or even with two prints flat. The aim is to reduce the overall procedure time but also to reach more possible locations for consultation using mobile solutions. Depending on the results, the persons can be the subject of a second line of consultation involving a full comparison of the ten prints flats and rolled. In all these cases, a live-scan is used.

Latent fingerprints. The identification of latent fingerprints in the context of a judicial procedure usually requires the "four eyes" principle (i.e. two different fingerprint experts have to agree on the final decision), however, in some Members States this procedure could include multiple steps involving up to seven fingerprint experts. The number of required minutiae to be used in court is typically 12 although this is highly dependent on the law of each Member State and this number can even go down to 8 if the minutiae points are sufficiently discriminatory according to the forensic experts [Ulery2014]. This dimension is not directly related to a possible implementation of an AFIS for SIS-II, however, it stresses the need for a high quality enrolment process so as to improve, in the best possible way, the results on queries using latents.

In addition, the storage of latent fingerprints triggers different legal issues, as the identity of the person to whom the latents belong is by definition initially unknown. This situation can lead to the storage within a criminal AFIS of latent fingerprints belonging to innocent citizens whose fingerprints were found at a crime scene (e.g. the latent fingerprints of a police officer who was inspecting the scene). Therefore, in the case of AFIS with a database of unknown latent fingerprints (also called unsolved case database), it is mandatory to have a common regulatory framework that defines a clear protocol specifying under what circumstances a latent fingerprint can be stored in the database and the procedure to follow when a hit is obtained from a search in this database. The MS visited have similar (still not equal) procedures and legal frameworks that regulate the use of latent fingerprint databases within their national AFIS. As underlined later in this report, currently, the SIS-II legislation does not foresee the storage of latent fingerprint.

AFIS performance assessment. Regarding the performance assessment of the national AFIS, different methodologies have been identified among the Member States. Broadly, performance evaluation strategies may be divided into three groups:

- Member States that do not carry out an independent evaluation of AFIS on their own real data (the final performance figures are those provided by the vendor);
- Member States that carry out their own assessment of the AFIS performance at the time of the call for tender or when the AFIS is first purchased; and
- Member States that perform independent evaluations of the AFIS, on a specific dataset containing real data, every time an update of the system is introduced.

It has to be underlined that conducting an independent benchmark of the performance of an AFIS is a costly and time-consuming action for which the benefits are not always immediately evident. The growing and relatively high maturity of the technology could also play a role in the lack of motivation for conducting such a task. However, where the result of such a benchmark leads to a higher performance of the system, the quality threshold for accepting fingerprints can possibly be lowered resulting in a wider identification capability.

4.3 Size of Member States AFIS

In this section, the main figures (only average numbers are given) related to the size of some of the national AFIS visited are provided. The aim is to give a concrete overall view of the AFIS already in operation. It should be underlined that for all of them, those figures such as the number of ten prints cards stored in the system are relatively stable over the year.

4.3.1 National criminal AFIS in France.

Last year, 900 000 dataset (ten print cards rolled and flat) were submitted to the national criminal AFIS by the 485 access points. The database contains around five million records rolled and flat. All of them are validated by an operator. Regarding latent fingerprints, the database contains 230 000 prints from unsolved cases and 140 000 were submitted to the system after having been processed and encoded by an expert.

4.3.2 National criminal AFIS in The Netherlands

With around 500 requests per day coming from 300 access points, the Dutch system provides a two-step approach: firstly, a fully automatized step uses ten prints flat. Secondly, in case of no hit, rolled fingerprints are used as well. The database contains 1.2 million records (ten print cards rolled and flat) and around 160 000 latent fingerprints from unsolved cases.

4.3.3 National criminal AFIS in Portugal

With around 14 000 ten print cards (rolled and flat) submitted every year, the central AFIS managed by the Ministry of Justice contains 237 000 ten print cards and around 200 000 latent fingerprints.

4.3.4 National criminal AFIS in Germany

The federal criminal AFIS stores around 3.2 million dataset (ten print card rolled and flat) and all of them have been manually validated before storage.The system is queried by 160 000 standard identification requests and 110 000 high priority requests called Fast ID (six flat fingerprints are used and a reply is expected within five minutes). The system also contains 422 000 latents from unsolved crime and processes every year 380 000 requests with latents (1200 per day).

SECTION 4. SUMMARY OF KEY CONCEPTS:

- From a technical perspective, the two main parameters defining the use-cases of AFIS are: the origin of the enrolled fingerprints in the AFIS database and the origin of the query fingerprints used to perform an identification.
- Three main types of queries are currently being implemented in most MS AFIS: full ten print searches, fast searches (using two-six live-scanned flat fingerprints), and searches using latent fingerprints.
- Different levels of human intervention (by expert forensic examiners) are implemented in MS AFIS. In general, this intervention level is very high in the case of latent fingerprint processing.

5 Non-Member States AFIS in production: illustrative examples

In addition to the nine Member States national AFIS (i.e. end-users of SIS-II), the JRC visited the United States of America (see Section 1.3.2) in order to gather information regarding the large- scale AFIS already being used in the country and which present significant similarities with an eventual AFIS which could be integrated in SIS-II. This information was complemented with further details obtained from other European AFIS already in production such as those in EURODAC or in the Visa Information System (VIS).

This section aims to provide the reader with an overview of the information related to these AFIS as they present significant similarities to the use and operational context of SIS-II. As in the previous section, the objective is not to give a detailed description of each AFIS, but to present a summary of their most relevant features so that the reader can build a general picture of the capabilities of AFIS technology today.

5.1 EURODAC

Launched in January 2003 in accordance with Council Regulation (EC) No 2725/2000, EURODAC is the oldest EU system offering an AFIS functionality. This Regulation establishes an EU asylum fingerprint database which aims to support the effective application of the Dublin Convention[14]. When someone applies for asylum, regardless of his/her location within the EU, his/her fingerprints (a ten print card) are transmitted to the EURODAC central system.

Reviewed in 2013, this Regulation has been replaced, since 20 July 2015, by Regulation (EU) No 603/2013[15] which introduced a series of new elements relevant for this report. In particular law enforcement access to the system is now allowed under certain conditions and latents can be used when querying the database.

According to the Annual Report 2014[16] produced by eu-LISA, EURODAC stores 2.7 million sets of fingerprints (ten prints flat) and a total of 756,368 transactions took place. The fingerprint rejection rate observed in 2014 was 4.49%.

EURODAC offers some interesting learning elements from the perspective of a SIS-II AFIS. Since 20 July 2015, searches with latents have been included and although there is not yet enough experience in its use, this system should be carefully monitored in order to obtain useful information to be applied to a future SIS-II AFIS. The size of the database is of a similar magnitude to SIS-II. However the volume of transactions is far smaller and the time-frame for dealing with requests is quite large (24 hours for a normal request and one hour for an urgent comparison).

5.2 Visa Information System (VIS)

In production since October 2011, the Visa Information System (VIS) allows the exchange of visa data between Schengen States. Around 12 million fingerprint datasets (flat ten print card) have been stored in the central database so far. In July 2015, the VIS roll out process reached 45%. Since October 2014,

[14] Regulation (EU) No 604/2013 of the European Parliament and the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)

[15] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013R0603

[16] http://www.eulisa.europa.eu/Publications/Reports/Eurodac%202014%20Annual%20Report.pdf

it is mandatory to conduct fingerprint verification at the first line of control at the border and in mid-July an average of 10 000 verifications (one to one) per day could be observed.

The system also offers an AFIS functionality, mainly used in the frame of new VISA applications or at the second line of control at the border with an average of 20 to 30 000 identification queries per day and a maximum peak/hour of 2600. According to the Service Level Agreement a reply to an identification query should be sent in less than ten minutes (less than three seconds for a verification with one to four fingers). Identification queries are conducted using a ten print card.

According to the VIS regulatory framework the three following cases of fingerprint processing are taking place:

1. In the course of a VISA application request, the fingerprint record is introduced and submitted to the VIS central system. The VISA applicant is enrolled and his/her fingerprints are checked against the database for possible duplicates/matches before completing the request.
2. The second case is the processing operation which takes place at the borders of the Schengen area with a verification and if necessary an identification using the AFIS functionality of the VIS at the second line for further checks.
3. The third case is a law enforcement access under the conditions foreseen by the VIS Decision. Contrary to EURODAC, the use of latent for these queries is not foreseen by the VIS legislation.

When this VIS rollout will be completed, up to 100 000 identification queries per day can be expected. During a VISA application process, a check against SIS-II is, in principle, also conducted. Today alphanumerical data are used for this check, but it is expected that fingerprints would be used if the SIS-II offers an AFIS functionality.

5.3 United States AFIS

The United States have deployed a series of AFIS in the multiple contexts at federal and State levels. The two biggest Federal systems are those from the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) which also seem to be the most similar to EU systems such as SIS-II. These two systems are briefly introduced below.

5.3.1 FBI: Next Generation Identification System

Initiated in 2007, the project for a Next Generation Identification (NGI) system of the FBI entered into production in September 2014 "*on schedule, under budget, with all objectives achieved*" as confirmed by the FBI during our visit. FBI biometric activity is based on more than 60 years of continuous investment and development with the NGI as the ultimate step. The database holds around 70 million records. Each consultation can lead to three possible scores: the best is fully automatic, the second will require the involvement of one examiner, and the lowest will require two examiners.

The overall architecture of the system is very similar to what might be expected in EU systems such as SIS-II: there are 50 access points to the NGI corresponding to the 50 States of the US. The way a consultation is processed will vary according to its nature: criminal (with priority) or civil. The processing always starts with a smaller part of the database comprising "the worst of the worst" (some nine million subjects related to the most serious crime). Compared to the previous system, NGI increased the accuracy from 96% to 99.6% (ten prints against ten prints) and, accordingly, manual review decreased by 90%.

In addition to the standard consultation (ten prints), a mobile solution (called RISC) for field officers was recently developed. It uses two fingerprints and is delivering three potential hit feedback within four seconds: red (between 3 to 7%), yellow or green.This consultation is only against the most critical criminal database. 22 States are participating so far with an average of 2000 searches per day.

NGI is also used for civil procedure such as the process of vetting persons in positions of trust (police officers, teachers, civil servant etc.). The service is charged to the organization requesting it.

The other new dimension of NGI is the introduction of new modalities: facial recognition is used against mugshots (20 million). In addition, the FBI has a centralised facial services unit aiming to pre-process the images received before submitting them to the system. Face is used just as a possible lead but not as evidence. An iris recognition-based system is also being used but so far only in the specific case of prisoner management during transfer.

The FBI claims to satisfy, with its central database, 60 different jurisdictions across federal states. Authorities in the federal states can access data stemming from other federal states only if the relevant laws allow it (a system quite similar to the links introduced in SIS-II).

The FBI also provides a centralised fingerprints laboratory based in Quantico where all the requests for latent fingerprint within the country are processed. Three possible consultations have been defined:

- a "quick launch" for which the possible minutiae of the latent are encoded automatically and then sent to the AFIS.
- a manual encoding for which an expert complements and validates the automatic encoding.
- a full manual encoding by an expert.

NGI is three times more accurate than the previous system. The examination of the list of candidates proposed by the system (usually ten) is done by two examiners (blind verification), and three main criteria are applied: quality, number of minutiae and surface. Around 100 latents/month are analysed by experts and 2000/month through the quick launch option (mainly for terrorist cases). From the total amount, around 18-20 per month are linked to missing persons (a type of alert also available in SIS-II). The system starts to list potential candidates with at least three minutiae. For a Unique Latent Matching, (formal identification), the USA does not apply any limit regarding the number of minutiae (In the EU it is between ten and 12 according to the MS visited).

The usage of Extended Feature Sets (EFS) for latent searches is envisaged for the future but is not yet implemented in the NGI AFIS.

5.3.2 Department of Homeland Security - Office of Biometric Identity Management

The Department of Homeland Security is managing a 130 million record AFIS database that provides services to a series of US agencies. Regarding the use of the DHS database at the borders, a Service Level Agreement sets out that fingerprint checks should not take more than 30 seconds during which a series of verification/identification transactions are conducted in the DHS as well as in the FBI database (10 seconds against the nine million "worst of the worst" records, 20 seconds against all other records).

Given the very large size of the database, a matching strategy has been defined and deployed based on a risk assessment approach. Using the information provided by the machine readable zone (MRZ) of a passport (alphanumeric search), the system checks if the person is already registered and, in that case, only a verification is performed. If the person is not registered, identification is performed against a limited list of the most wanted persons as a first action and the process is accelerated by again using the information provided by the MRZ such as the age, the gender etc. Fifty different types of cases/alerts can lead to an enrolment, among them there is the possibility to "flag" only, essentially an "attention drawn" message (similar to Article 36 of SIS-II Decision related to persons for discreet or specific check). The quality threshold is deliberately maintained at a relatively low level according to DHS representatives met. In the case of a hit, the person goes to a second line of check.

Further checks with a faster response time but with a much lower risk are also performed after the person has left the check point. Around 300 000 consultations are conducted every day.

SECTION 5. SUMMARY OF KEY CONCEPTS:

- There are already large-scale AFIS in operation in the world. Some of the use-cases and features of these AFIS are similar to those which can be expected for the SIS-II AFIS.
- Most national AFIS conduct searches on databases of more than five million records.
- There are already large-scale AFIS that can process over 10 000 consultations per day.
- In the case of AFIS working with a large database and processing a large volume of queries, it is important to define a specific matching strategy according to a priority or risk assessment of the different types of query.

6 Lessons learned: challenges faced by AFIS technology

All the information regarding AFIS technology gathered during the five initial phases of the project (see in Section 1.3) has allowed to identify the different challenges currently faced by this type of system including in implementation. Such challenges, which in many cases are intertwined, can be summarized as follows:

- **Use-cases**: probably the most critical parameter in the design of an AFIS is the definition of the use-cases, scenarios and operational context in which the system will be used. These use-cases will determine, to a large extent, the type and number of enrolment/consultations that the system will have to support and, therefore, all the other parameters listed below are somewhat linked to this one.
- **Performance**: this feature refers to the accuracy of the system, that is, its ability to find in a given database the queried identity. Very high performance becomes especially critical in the case of AFIS that have to cope with large databases.
- **Quality**: this feature refers to the biometric quality of the fingerprints that are processed in the system. Ensuring high quality, especially of the samples enrolled in the database, is a critical parameter in order to achieve a high level of performance.
- **Integrity of the database**: this feature refers to the correctness of the data stored in the AFIS database. Typical errors that are usually observed in AFIS databases include: doubled fingerprints, mixed fingerprints (e.g. an index finger that is labelled as ring finger), fingerprints not corresponding to the right person, incomplete ten print cards, missing fingerprints, inconsistency between alphanumeric data and fingerprint data etc. It is absolutely critical for the correct functioning of an AFIS to mitigate, as much as possible, this risk.
- **Type of data being processed**: with regard to the use-cases, it is important to define the type of fingerprint data that the system will have to work with in enrolment, consultation and test. For instance, possible types of fingerprints are: flats/rolled, live-scanned/inked/latents, individual/ten prints etc. The quality of the different type of data differs significantly and therefore it also has an impact on the final performance of the system.
- **Latent fingerprints**: they are probably the biggest challenged face by current AFIS due to their anticipated very low quality. Defining a specific processing strategy for this particular type of data (i.e. fully automatic, partially assisted etc.) is usually required to obtain the expected performance standards.

In addition, the storage of these data triggers different legal issues, as the identity of the person is unknown. This situation can lead to the storage within a criminal AFIS of latent fingerprints belonging to innocent citizens whose fingerprints were found at a crime scene. Therefore, in the case of an AFIS with a database of unknown latent fingerprints, it is mandatory to have a common regulatory framework that defines a clear protocol specifying under what circumstances a latent fingerprint can be stored in the database and the procedure to follow when a hit is obtained from a search in this database. Although consultation using latent fingerprint is included in the SIS-II legislation their storage is not.

- **Speed**: this feature refers to the response time of the system when a query (i.e. consultation) is launched. The response time can be a critical parameter for certain use-cases where the time constraints are very strict (e.g. first line border control).
- **Size of the database**: this refers to the number of identities enrolled in the system database and which will be used to perform the searches. This parameter is one of the key design features and should be carefully estimated before putting in place any AFIS. The size of the database will have a big impact on the response time of the system and is one of the features to be taken into account when defining the minimum performance expected for the system.

- **Number of transactions at peak hours**: together with the database size and the expected response time, this feature is also a key design feature to size the AFIS (in terms of the necessary processing power). It refers to the number of consultations that the system will have to process and, as in the case of the database size, it should be carefully estimated in the design phase.
- **Matching capacity**: this feature is totally linked to the previous one (i.e. number of transactions). It refers to the number of matchings (i.e. comparisons between individual fingerprint samples) that the system should be able to perform at peak hours. This parameter is required, as each different type of transaction may imply a different number of matchings.
- **Strategy to handle the queries**: although this may be considered a secondary feature it may play a very important role in the transaction response time and therefore in the resources needed by the AFIS. For instance, in many cases, it is useful to assign a priority to each transaction depending, for instance, on the expected response time.
- **Exchange formats**: it is essential to define a unique, standardized exchange format for the different type of data handled by the system (e.g. fingerprint images, fingerprint templates, scores etc.)
- **Multiple fingerprint records**: the possibility to store multiple fingerprint records could offer the possibility to apply an improved quality strategy such as using the best record or produce a composite ten print record with the best available fingerprint images. The strategy may vary according to the fingerprint submitted for consultation (latent or ten print).
- **Operational procedures**: in some AFIS users follow different operational procedures to interact with the system (e.g. fingerprint acquisition methodology). Although such diversity is not crucial for the successful integration of an AFIS, it can have a negative impact on its accuracy. Therefore, it is preferable to work towards the harmonization of such methodologies and their best practices in order to achieve the maximum possible performance of the system.
- **Human intervention**: although representing a decreasing part of the overall, process thanks to performance improvement in biometric technology, manual processing remains an important step in some uses-cases and should therefore be optimised.
- **Maintenance and performance evaluation**: benchmarking the performance of an AFIS is a healthy and important task to be conducted during the life-cycle of a biometric system. This task not only provides important information on the performance of the system in production (with real data) but can also be a useful tool for fine-tuning the system and eventually improve its performance.
- **System architecture**: all the previous technical features, as well as other parameters derived from the specific context (e.g. political) in which an AFIS will be deployed, should be taken into account during the design phase in order to select the most suitable architecture (e.g. distributed, centralized, hybrid).

The aim of the next part of the report will be to detail and address these challenges, whenever possible, in the context of SIS-II and its potential AFIS functionality.

This page is intentionally left blank.

PART II: THE AFIS IN SIS-II

PART II of this report is focused on SIS-II and its future AFIS functionality. This part refers to and builds upon many of the concepts, terms and general aspects of AFIS technology already described in PART I. PART II is based on the following rationale:

Firstly, taking into account its legislative framework, a description of the key aspects concerning SIS-II today (i.e. with no AFIS integrated) is presented.

Secondly, according to the challenges exposed in Section 6 (PART I) and to the specificities of the SIS-II described below in Section 7.1 (PART II), a series of recommendations are set out on how to tackle such challenges in order to implement an AFIS in SIS-II in the most effective manner.

Thirdly, adopting a more prospective view which goes beyond today's regulatory framework, we describe some possible functionalities that could be further added to SIS-II in order to improve its utility and accuracy and provide consolidated services.

Fourthly, we present the final conclusions of the report.

7 The Schengen Information System II

In order to put the potential SIS-II AFIS into perspective, EU large-scale biometric systems, national AFIS and US AFIS have been described in the report primarily with the aim of more accurately understanding the nature and volume of processing operations which can be envisaged for a SIS-II AFIS. In this section, we present, first of all, the main facts describing SIS-II today. Then, a series of use-cases, which can be foreseen by SIS-II regulatory framework, is described and compared with those previously introduced.

7.1 SIS-II today

As already introduced in Section 1.1, SIS-II was launched with a double intention: to contribute to law enforcement cooperation between the Member States and support external border control. Police and border guards are able to enter and consult alerts on certain categories of wanted or missing persons and objects. SIS-II consists of three major components: a central system (CS-SIS-II), national systems which may contain a synchronised copy of the central system and a communication infrastructure (network) between the central system and the national systems.

The SIS-II central system, managed by the EU agency eu-LISA, is where all the alerts produced by the Member States are stored. A real-time updated copy of the central system can be maintained by each Member State, according to Article 4 of SIS-II legislation. Some Member States have a partial copy comprising only the alphanumeric data of the alerts, others have a full copy including face and fingerprint images[17].

According to the annual and detailed reports produced by eu-LISA[18], SIS-II contains today 61 million alerts and only 1.43% of those alerts are related to persons (slightly less than 800 000 on 1 January 2015, as presented in Figure 7. As will be underlined later, this is a relatively small amount compared to the national AFIS visited in the course of this study (see Section 5). Even if it is already allowed according to Article 22, not all of these alerts will lead to an upload of fingerprints. Indeed, fingerprint data corresponding to the person related to those alerts are not always available.

On the other hand, the volume of consultations can be considered very large, with almost two billion queries in 2014 but with only 350 million of them directed to the central system, which handles around 20% of the overall transactions. The other 80% of transactions (i.e. 1.65 billion) are processed through national copies. As will be discussed later, these figures refer to the *total* number of queries including *all* alerts, not just those alerts related to persons which are the only alerts that could potentially have fingerprints associated with them.

[17] It can be noted that fingerprint template interoperability does not constitute an issue within EU systems like EURODAC or VIS as these systems were designed to only accept fingerprint images as input. In case the AFIS provider changes, the fingerprint images are simply "re-coded" into the new templates of the new AFIS provider. This is possible only if the system is a lights out system with no human intervention for the encoding phase (which is not usually the case for latent fingerprints).

[18] http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx

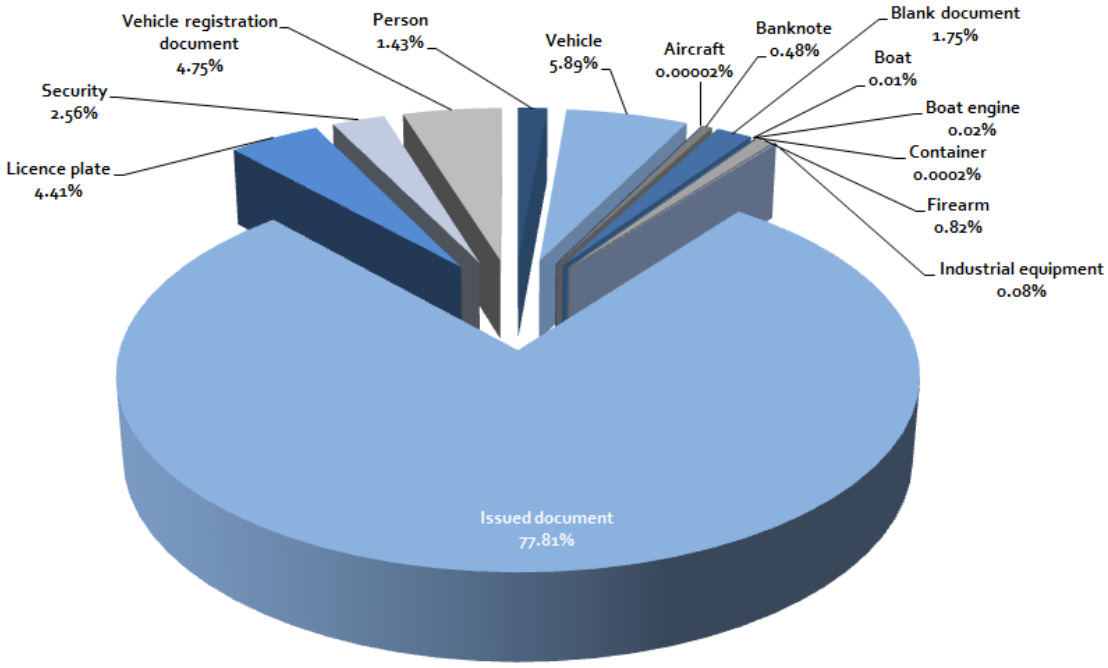

Figure 7. Distribution of alerts in SIS-II in 2014 (source eu-LISA)

7.2 Fingerprints use-cases from the SIS-II Regulation and Decision

A prerequisite for an accurate assessment of "*the availability and readiness of the required technology*" is a proper identification of possible use-cases involving the automatic processing of fingerprints. In this section we discuss the use-cases which have been identified from the SIS-II Regulation and Decision.

The aim is to compare the use-cases offered by the SIS-II regulatory framework for which fingerprints will be processed with those developed at national level in the framework of law enforcement and border management activities identified in Section 4.1. Logically it is expected that the solid expertise built at national level over a long period of time will be applied, whenever possible, to the development of the use-cases offered by a potential SIS-II AFIS.

The SIS-II regulatory framework provides a series of actions for which fingerprints might be processed. Two main categories of use-cases can be foreseen regarding the processing of such data:

- **CUD transactions**: An alert is the subject of Creation/Update/Delete (CUD) action during which fingerprint will be processed, enrolled, updated or deleted from the AFIS database. Therefore all these operations can potentially entail a change in the AFIS database.
- **Consultations**: The SIS-II database is consulted using fingerprints, that is, the AFIS is used to launch a search on the fingerprint database looking for a given identity (i.e. subject). In these operations no modification is performed in the fingerprint database.

It should be underlined that a consultation will take place, in any case, prior to a CUD of an alert (creation operation in particular) in order to detect if this new alert might be related to the same person of another alert which has already been introduced. The Member State which is entering this new alert then has the possibility to create a link with these existing alerts in conformity with Article 52 of the SIS-II Decision.

7.2.1 Issuance of new alerts

The SIS-II Regulation and Decision offer Member States multiple possibilities for introducing new alerts in the central system and some of these alerts relate to persons i.e. third country nationals and EU citizens. As detailed previously, for a total of 61 million alerts, slightly less than one million relate to

persons. According to the 2014 statistics, around 17 million CUD (Creation, Update and Delete of alert) transactions took place and 1.4 million of those transactions were related to persons.

Although fingerprints are not on the mandatory list of data required for creating an alert, whenever available they shall be entered. The following list of cases corresponds to the possible alerts Member States can process (CUD) using fingerprints.

7.2.1.1 Case A: Refusing entry and stay (Regulation, Article 24)

According to the SIS-II Regulation, an alert can be issued for the purpose of refusing entry and stay to third country nationals. This type of alert is by far the most frequent related to persons with 68.56% of the total. Assuming that a Member State issuing the alert has access to the third country national who is the subject of this alert, ten prints will be collected (preferably rolled and flat, see Section 8.6), added to the alert and eventually compared with the ten prints cards already introduced in the SIS-II database which might lead to the creation of links with other alerts, whenever it is allowed.

Case A is covered by the technical use-case 1 (ten print vs ten print) described in Section 4.1.1.

7.2.1.2 Case B: Misused identity (Decision, Article 51)

According to the SIS-II Regulation and Decision, with the consent of the data subject whose identity has been misused, Member States can introduce, among other personal data, the fingerprints of the victim of the misuse, to the alert related to the person who misused this identity. This measure, which will lead to an *Update* of an alert and not a *Creation* per se, will allow the authorities to distinguish between the impostor and the victim, as the victim can prove his/her identity whenever necessary. Today, after a possible hit from an alphanumeric search at the first line of control at the border, the identity of the victim can be verified and confirmed at the second line of control.

Case B is covered by the technical use-case 1 described in Section 4.1.1. (ten print vs ten print). A ten print card will be introduced and also compared at a later stage only with the ten print cards already stored under the related alert in the system.

7.2.1.3 Case C: Arrest for surrender or extradition (Decision, Article 26)

According to the SIS-II Decision, a Member State issuing an alert related to a person wanted for arrest for extradition or surrender purposes on the basis of a European Arrest Warrant has the possibility to complement the alert with fingerprints when they are available. In principle, the person subject of this alert might not be accessible at the time of the issue of the alert and fingerprints will not be available. However, it might be possible that the Member State issuing the alert already has, in its national AFIS, the fingerprints of this person and is therefore in a position to complete the alert with these data. Ten prints will be collected, added to the alert and eventually compared with the ten print cards already introduced in the system for possible additional links with other alerts. It is also possible that the subject of this new alert has been already the subject of another type of alert for which the fingerprints have been collected.

Case C is covered by the technical use-case 1 described in Section 4.1.1. (ten print vs ten print). According to part 2.13 of the SIRENE Manual[19] these fingerprints can also be provided by another Member State.

7.2.1.4 Case D: Missing persons (Decision, Article 32)

According to the SIS-II Decision, Member States can issue alerts on missing persons. In principle, the fingerprints of these persons are not always available when the alert is created. However, in certain cases, if a national registry is available and if national legislation allows it, fingerprints can be transferred from this registry to the alert. Also, in the course of the investigation, latent fingerprints

[19] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D0219&from=EN

of the missing person may be used to query the database (not to be stored in the database), then it is no longer a CUD transaction but a consultation case described in Section 7.2.2.

Depending on the exact situation described above, Case D is covered by technical use-case 1 (ten print vs ten print) described in Section 4.1.1.

7.2.1.5 Case E: Persons sought to assist with a judicial procedure (Decision, Article 34)

According to the SIS-II Decision, Member States can issue new alerts on persons involved in a judicial procedure, such as, a witness who has to attend a criminal trial. Like case D, fingerprints might not always be available; however, whenever it is the case, Member States can complement the alert with them even from their own national AFIS database. Those situations might trigger issues related to the format of available fingerprints which may not be fully compliant with the SIS-II format.

Depending on the scenario, Case E is covered by technical use-case 1 (ten print vs ten print) described in Section 4.1.1

7.2.1.6 Case F: Discreet or specific checks (Decision Article 36)

According to the SIS-II Decision, Member States can issue alerts on persons in the context of prosecuting criminal offences and for the prevention of threats to public security. Here again there might be cases where fingerprints are not available. The nature of the checks (see Section 7.2.2 on consultation) implies that, in principle, fingerprints are not likely to be accessible at a later stage or at least it is not probable that a full ten print card will be collected. However, border checks might offer the possibility to collect these fingerprints and complement the alert introduced by another Member State or at least, in a case of discreet surveillance, to conduct a simple check.

Depending on the scenario, Case B is covered by technical use-case 1 (ten print vs ten print) described in Section 4.1.1.

7.2.2 Consultation of the SIS-II database

As defined by the SIS-II Decision and Regulation (Article 40 and Article 27), several authorities have the right to access and consult the alerts stored in the system. Almost all the technical cases defined in Section 4.1 will cover the range of possible consultations and therefore usages of a possible SIS-II AFIS. The last two technical use-cases defined in Section 0 (latent vs latent) and 0 (ten prints vs latent) will not be part of those possible consultations under the existing SIS-II regulatory framework which does not foresee the possibility to store such data within an alert.

Today those consultations are carried out using alphanumeric data and take place in activities such as investigation and prosecution, border checks, VISA and asylum processing operations.

When the AFIS functionality is implemented all the possible alerts listed in the previous section which are related to a person (case A to F) might be the subject of a consultation such as ten print vs ten print (technical use-case 1), two print flat vs ten prints (technical use-case 2) and latent vs ten print (technical use-case 3).

8 Facing AFIS implementation challenges: Recommendations

Following the different challenges identified in Section 6 related to the implementation of large scale AFIS, and given the specificities of SIS-II described in Section 7, a general view on how those challenges may be addressed for the SIS-II context as well as different options for the actual design and use of the envisaged AFIS functionality are presented in this section. Some practical recommendations are also given. In some cases, those challenges identified in Section 6 that are very much intertwined have been grouped into the same subsection.

8.1 Size quantification of the SIS-II AFIS: database and volume of transactions

As defined in the AFIS challenges described in Section 6, the size of an AFIS is determined mainly by two main parameters:

1. Size of the Database with all the fingerprint records on which searches will be conducted,
2. Volume of transactions to be processed by the AFIS.

Both parameters are quite independent as there are already working systems with small databases and a very large volume of transactions and others with very large databases and limited transactions.

The current statistics on the use of SIS-II (some of which were already provided in Section 7), allow us to make a first overall estimation of the size of the SIS-II AFIS both in terms of database size and of volume of transactions. The next subsections give this initial view of the AFIS size.

8.1.1 Size of the SIS-II AFIS database

As already stated earlier, there are slightly than one million alerts related to persons. This number seems to be quite stable over time with only a slight variation. If for all these persons, fingerprints were available and attached to an alert (by September 2015 slightly less than 97 000 sets of fingerprints had been introduced), the size of the necessary IT platform to support such an AFIS would not exceed the size of the different national AFIS visited. Some of the AFIS used in large Member States contain ten times more data (as described in Section 4).

As confirmed by the Member States, the relatively small number of fingerprint records already stored in SIS-II is mainly due to the absence of an AFIS functionality. It can therefore be expected that the number of fingerprints will considerably increase as soon as this functionality is implemented. In the light of the relative stability in the number of records stored in the respective national AFIS, it can be expected that the number of alerts related to persons will be relatively stable in the long run. A slight increase in the number of alerts related to persons might however be observed at the beginning of the introduction of the AFIS functionality as it will raise new interest in creating alerts which will have a better chance of a possible hit with such a functionality.

8.1.2 Volume of transactions for the SIS-II AFIS

The elements contributing to the quantification of the number of transactions to be processed by the future SIS-II AFIS can be grouped into the three following categories:

1. ***Consultations which are already sent to the SIS-II today and will be supported most probably by the AFIS:*** considering that new VISA applications should be checked against SIS-II (see Section 5.2), it can be already assumed that up to 100 000 identification queries per day will be conducted in the future SIS-II AFIS from consular posts. Similarly, according to the 2014 report, the EURODAC system processed 750 000 transactions and, prior to these transactions, the VIS system as well as SIS-II shall be consulted for the purpose of the prevention, detection

and investigation of terrorist offences and other serious criminal offences. As soon as the AFIS is available it can be assumed that those consultations will also be based on fingerprints complementing the alphanumeric data. Last but not least, checks at external Schengen borders lead, in principle today, to an alphanumeric consultation of SIS-II which could, later on, also be complemented by a fingerprint check. For the volume of those possible border checks two sources are available today: the 2015 Risk Analysis report of FRONTEX[20] where the last available passenger flow mentions 700 million for 2011, and the Technical study on Smart Borders published in October 2014 which forecasts 550 million border crossings[21] for 2014.

2. ***Elements which could further increase the volume of transactions:*** as confirmed by all the Members States consulted, the introduction of an AFIS will greatly improve the attractiveness/usefulness of the consultation related to persons. This new functionality could also in itself potentially increase the number of new alerts created which are related to persons.
3. ***Elements which could decrease the volume of transactions****:* as already underlined, not all the alerts related to persons can be complemented with fingerprints (i.e. in some cases the fingerprint data may not be available). The availability of fingerprints is not a pre-requisite for the introduction of an alert related to a person according to Article 23(1). Accordingly, not all the queries related to persons can be conducted using fingerprints, such as in the case of missing persons or in some situations related to discreet surveillance. It has to be noted that, under strict conditions, for those Member States having a national fingerprint registry, it is possible to conduct searches on missing persons using the fingerprint records registered in their national database.

Quantification of the required transaction capabilities is much harder to predict at this point than the size of the database. This assessment depends on the identified use-cases, the number of access points (which can vary from 500 000 to one million for SIS-II) as well as the volume and frequency of those transactions. A reasonable starting point for an initial estimation is the number of operations related to persons from the total number of queries performed in the SIS-II today, comprising: 1) the processing of alerts (CUD) and, 2) the consultations (i.e. searches on the database). A first estimation of these two figures is given below.

8.1.2.1 CUD transactions

As introduced before (see Section 7.1), according to the annual report provided by eu-LISA, the processing of alerts (CUD) has generated 1.4 million transactions related to persons in 2014. Among these CUD, around 780 000 were related to the Creation, Update and Delete of alerts on persons for which a fingerprint processing (check) operation can be potentially expected.

8.1.2.2 Consultation transactions

The largest percentage of transactions using the AFIS functionality will come from the database consultations in SIS-II. In 2014 almost two billion queries have been sent to SIS-II with 20% of them to the central system and the rest to the national copies managed by Member States. Of course, not all those consultations (around 350 million in 2014 for the central system) were related to persons but unfortunately this specific statistic is not directly available today. It is also true that not all the consultations related to persons will be introduced using a fingerprint, but Member States clearly confirmed that whenever possible in the sphere of law enforcement or border check activity the functionality will be used in a fast way (two prints) and/or exhaustive way (ten prints).

[20] http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2015.pdf

[21] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/smart_borders_report_/smart_borders_report_en.pdf

RECOMMENDATION 1: Need for complementary statistics

- We recommend that, following a consultation with the EDPS by the Commission, eu-LISA identifies the best possible ways to include in its statistic annual report the number of consultations per year related to persons. In order to complement this assessment at central level, we also recommend that Member States report annually on the number of consultations related to persons that have been carried out on their national copies and, whenever possible, on the context of these consultations (e.g. at the police office, at border check).

8.2 Use of the SIS-II AFIS driven by national AFIS expertise

Since the AFIS functionality of SIS-II will be used following methodologies comparable to other fingerprint-related national tools for law enforcement, it is expected that similar levels of information will be provided and handled. This would imply, as is already the case at national level, the inclusion of all fingerprint types (i.e. flat/rolled, live-scanned/inked and latents).

RECOMMENDATION 2: Promotion of best practices

- We recommend that the expertise acquired during the development and management of national AFIS is appropriately applied to the SIS-II AFIS deployment and that best practices identified at national level are further fostered.

8.3 Common exchange formats

The SIRENE Manual (part 2.13.5) requires a check at national level regarding the compliance of fingerprints to be uploaded to the system with the ANSI/NIST-ITL 1-2000 specified format. However, it seems that there is still some diversity between Member States on how the sets of fingerprints have to be encoded, stored and transmitted.

RECOMMENDATION 3: Common exchange standard

- So far, NIST containers, as required by the SIRENE Manual and the best practice guide from Interpol[22], seem to provide an appropriate basis regarding the exchange of fingerprint data. We recommend that an automatic check for their mandatory and complete implementation should be developed in order to appropriately support the deployment of the SIS-II AFIS functionality.

8.4 Use and possible overlap with other systems

All visited law-enforcement entities agreed that there is an urgent need for an AFIS functionality to be implemented in SIS-II. Having access only to alphanumeric data greatly limits the potential use of the system and its added value compared to systems like Prüm.

It was noticed that the perspective of the Members States regarding the SIS-II AFIS evolved in the course of the visits. In most cases, at the beginning of the visit, the possible overlap between the two systems was underlined by the law enforcement officers. However, in the second and last part of each visit, Member States perceived, in a clearer way, the specific added value of a possible SIS-II AFIS and concluded that this functionality could become a good Prüm partner.

RECOMMENDATION 4: Prüm and SIS-II complementarity

- A need for clarification between the functionalities of Prüm system and of a future SIS-II AFIS was strongly identified during the visits. We recommend that this need is addressed.

[22] Guidelines concerning Fingerprint Transmission. INTERPOL OS/FTD/IDFP (2012)

8.5 Architecture

The challenge of the future AFIS architecture supporting SIS-II should be addressed in two spheres: the interaction between the Member States and the central system, and the internal organization of the system itself. The options suggested below mainly illustrate the first sphere. The second sphere will only be tackled briefly as it will, in principle, be the subject of a targeted and deeper IT technical analysis conducted by eu-LISA which is in charge of the management of such systems and has the responsibility of updating, whenever needed, the Interface Control Document (ICD) of SIS-II, describing in full technical detail the possible interactions between the central system and the Member States.

The options suggested by the JRC, as well as any other potential choices for the possible architecture of the SIS-II AFIS functionality, will have to at least take into account the following elements:

- The current architecture of SIS-II is composed of a central system dealing with 20% of the queries and of national copies which can be partial, with only alphanumeric data (nine Member States have such copies) or complete, (16 Member States are in this position) with the biometric data (image of face and fingerprints). The five remaining Member States have only direct access to the central system. Accordingly, 80% of the queries are processed using the national copies. **In the light of this situation we can conclude that an AFIS at the central system is required, in order to provide first this functionality to the Member States which do not have national copy or only a partial copy, and second to the Member States which might face a temporary technical issue with their national copy.**
- All Member States use the central system for Creation, Update and Deletion (CUD) of alerts. The introduction of an alert will require, as a matter of consistency, a quality check at the central system operated by the AFIS. Any processing of an alert (CUD transaction) sent to the central system is then broadcast, within three minutes maximum, to the existing national copies. **An AFIS will, therefore, be necessary at central system level for CUD processing operations.**
- According to Article 9(2) of SIS-II regulatory framework, a search in a national copy shall produce a result equivalent to that of a search in the SIS-II database. The necessary compliance with this article for alphanumeric searches will have to, in principle, also be applied for fingerprint searches. **A SIS-II AFIS running on a SIS-II national copy will have to offer the same identification results (accuracy, behaviour) as that running on the central system.**

Taking into account the elements listed above, it can already be concluded that an option proposing the use of existing national AFIS for querying national copies could be legally uncertain as it would not be in compliance with the SIS-II regulatory framework. If this option were allowed, it will no longer be possible to guarantee that equivalent results for a query in the central system and a national copy will be obtained.

8.5.1 Option 1: A unique AFIS running on SIS-II central system only

As presented in Figure 8 below, it is envisaged in this option that the SIS-II AFIS functionality would only be provided by the SIS-II central system. Member States B with a full national copy would query the central system whenever they need to conduct a fingerprint identification. However, for a manual confirmation of a result (in principle a hit) to be conducted by a dactyloscopic expert, the fingerprint images also stored in the national copy might be used in order to limit the traffic with the central system.

The other Members States A and C, having only alphanumeric data or even no national copy, would fully rely on the SIS-II AFIS of the central system.

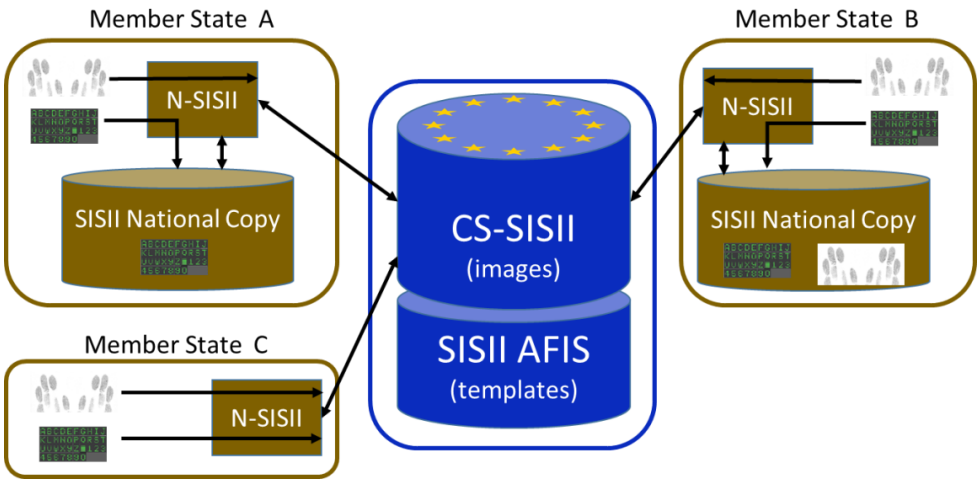

Figure 8. CS SIS-II AFIS only

The national copy contains only images of fingerprints. The central system, supported by the AFIS functionality, would also store templates of the fingerprints (encoded fingerprints).

8.5.2 Option 2: A unique AFIS running on SIS-II central system and national copies

In order to offer a complete decentralized solution to the Member States which already have a full national copy, the "hybrid "option described in Figure 9. CS SIS-II AFIS + National SIS-II AFIS can be proposed.

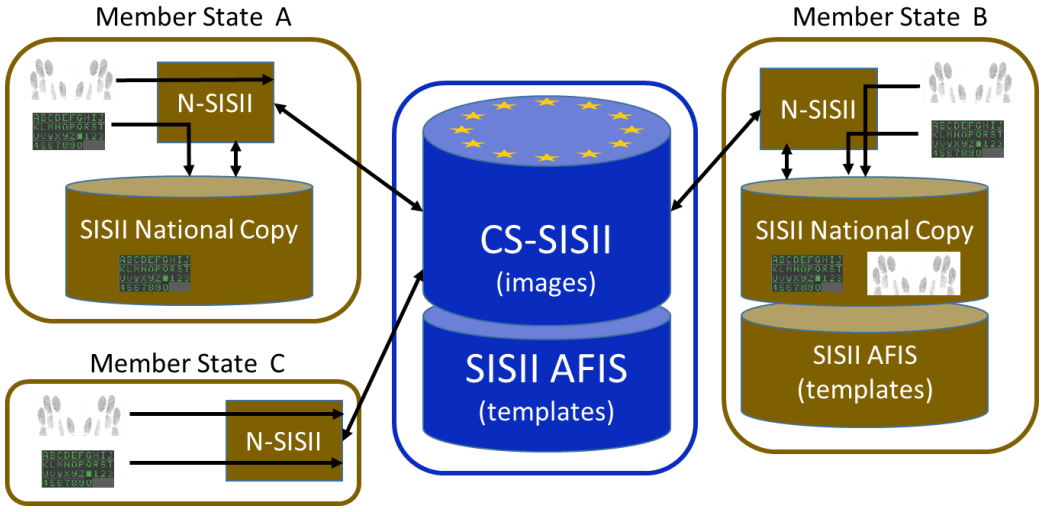

Figure 9. CS SIS-II AFIS + National SIS-II AFIS

With this architecture option, any technical update of the central system SIS-II AFIS functionality would also be broadcasted to the Member States having a full national copy and the same national SIS-II AFIS functionality so as to guarantee the consistency of results at national and central level. Such broadcasts would take place in addition to the synchronization of the central database with the national copies. This principle is equivalent to an anti-virus solution implemented in an organization where a central server keeps up-to-date the anti-virus running on each client machine of the corporate network.

With this option, it would also be possible for Member State B to have a full national copy (with fingerprint images) and still query the central SIS-II AFIS. This option would offer the advantage of distributing the processing power required by matching processes triggered by consultation and CUD

operations. Like the previous option, Member State A & C, with only partial copy or no copy, will use the central system SIS-II AFIS.

8.5.3 Internal architecture of the AFIS

As soon as the option for the overall architecture has been selected and defined, a targeted analysis will have to be conducted so as to define the best possible choices from an IT point of view and introduce them, in detail, in the new ICD of SIS-II. However, in the light of the national AFIS visited, some preliminary points can already be suggested for this stage.

A dedicated sub-system for searches involving latents could, for example, be proposed as well as another for fast identification queries leading to hit/no hit replies only. Possible synergies with other large-scale IT systems, in order to obtain higher efficiency and cost effectiveness, can also be foreseen: a sub-system dealing with latents could, for example, be shared with other systems also requiring this functionality, such as EURODAC, without compromising the data from each system which are kept separated. It could even be considered to use the best possible AFIS algorithm for each category of query: following a performance benchmark analysis, the best AFIS for latent search and for ten print searches would be selected.

RECOMMENDATION 5: Dedicated sub-systems

- In order to better respect the different business cases envisaged for a SIS-II AFIS, we recommend to consider in the design of such a system the use of dedicated sub-systems for each category of query.

8.6 Enrolment

To a certain extent, it can be considered that enrolment phases are already conducted in the SIS-II as some Member States have uploaded fingerprint images in the central system (around 97.000 by September 2015), but as pointed out in the next section, some critical parts of this enrolment are still missing. In any case, the future AFIS functionality will have to deal mainly with two possible situations:

1. enrolment phase with the data subject available.
2. enrolment phase supported by information extracted from previous enrolment data stored in other systems.

RECOMMENDATION 6: High-quality enrolment process

- We recommend that, whenever a data subject is available, that is, in most of the cases, the enrolment phase should favour the use of live-scan devices and be conducted under the control of experienced operators, as is usually the case in a law enforcement context. This should result in the production of a high-quality ten print card containing both rolled and flat data.

As observed in most of Member States national AFIS, multiple records from the same person are stored in the database and can cover, in some cases, a relatively long period of time. Four datasets have been usually observed. The benefits of such storage are twofold. Having several datasets from the same person offers the possibility of increasing the performance of the matching process by selecting the fingers with the highest quality score. Basically, the AFIS application builds the best possible ten print card (known as a composite ten print card) from the prints available in the system and, of course, belonging to the same person. The second possible added value for keeping several datasets is the potential improvement for latent matching processes. Even if some of the fingerprints of those datasets did not reach a satisfactory quality score and will not be selected for a ten print card matching process, they might present unique features which will produce a hit from a latent matching process.

RECOMMENDATION 7: Storage of multiple datasets

- We recommend to envisage the storage of multiple datasets (e.g. four datasets) for a SIS-II AFIS to support a composite matching strategy. As long as it is clearly established that the datasets belong to a same person, a composite check would be the result of multiple datasets associated with a single alert or datasets belonging to several alerts, which should already benefit of links established in accordance with Article 52 of the SIS-II Decision.

Figure 10 summarizes the possibilities for enrolment in the context of law enforcement activities in addition to the consultation possibilities further explained in Section 8.8.

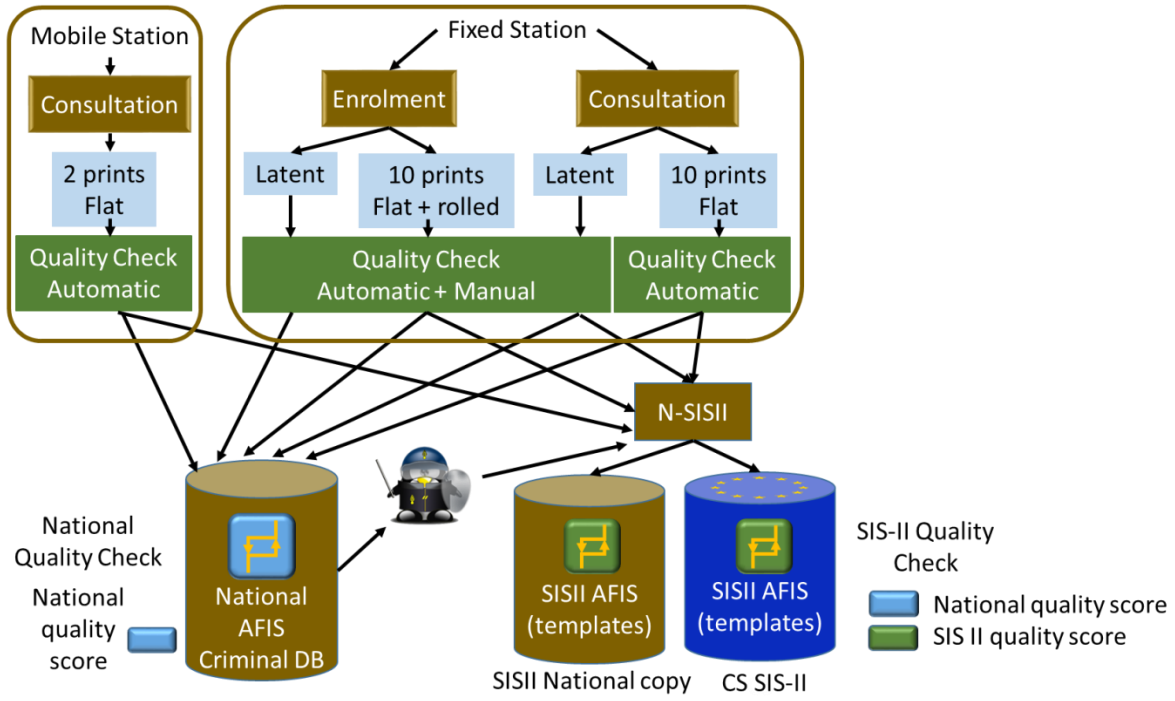

Figure 10. Law enforcement

When the person, subject of a new alert, is not available to the authority that will introduce the alert, it might be possible that fingerprint records belonging to this person are technically and legally available in some other national system such as a criminal AFIS or a national registry. As foreseen in the SIRENE Manual part 2.13, these fingerprints can also be provided by an authority in another Member State. In both cases the fingerprint datasets might not fulfill all the quality and presentation standards required for a full enrolment in the SIS-II AFIS. They might, for example, be only flat prints and the quality may have been computed by a different system.

RECOMMENDATION 8: Controlled transfer of datasets

- We recommend that SIS-II AFIS accepts fingerprint datasets produced via other systems, as long as the parameters of these systems are kept in the dataset included in the alert. NIST containers offer the possibility to keep several quality scores issued by different systems.

8.7 Quality

As emphasised strongly throughout the report, quality should be considered as the main key success factor for an efficient deployment of the SIS-II AFIS. Below we propose a series of recommendations aiming to control, to the largest possible extent, biometric sample quality. Three points of action have been identified:

- the capture point (a critical point of action because it acts as the main interface between the user and the system) which has already been partially covered in Section 8.6 related to enrolment,
- the quality assessment algorithm,
- the system performing the recognition.

As already mentioned in Section 3, improved quality, by either capture point design or system design, will lead to better performance. Some of the identified measures to improve quality include, for instance, initiating reacquisition from a user, selecting the best sample in real time or selectively evoking different processing methods.

8.7.1 Capture point

RECOMMENDATION 9: Quality of capture points

- **Supervision by an operator.** Adequate operator training is recommended, as supervision of biometric acquisition is a repetitive task and requires additional attention in the case of centralised enrolment stations. The aim is to avoid tiredness and boredom adversely affecting the process.
- **Adequate sensor.** We recommend to use performant fingerprint sensors (e.g. in size and resolution), offering also enhanced capabilities to acquire low-quality sources. Whenever possible live-scan devices should be favoured for capturing fingerprints.
- **Enhanced graphic user interface (GUI).** We recommend that capture points have large displays and provide real-time feedback of acquired data.
- **Proper user interaction.** The enrolment process should be user-friendly with clear procedures which are properly explained. The use of good ergonomics should support better acquisition practices.
- **Adequate environment.** The acquisition environment should be appropriate in terms of illumination, temperature and backgrounds both for the subject and the operator. These elements are recommended mainly for fixed stations but similar considerations are instrumental as well for mobile stations.
- **Sensor maintenance.** There should be regular and systematic cleaning of the enrolment stations to avoid “ghost fingerprint” effect, especially in the case of consultation processes taking place in heavily used check points.

8.7.2 Assessment algorithms

RECOMMENDATION 10: Quality assessment algorithms

- **Adherence to standards.** We recommend to include in a SIS-II AFIS the results of the quality metrics algorithm used locally by Member States as well as the results of the use of standard quality metrics such as NFIQ and NFIQ-II. These two results will complement those provided by the quality metrics algorithm of the SIS-II Central AFIS functionality. All three results can be added in a single NIST container, as for ANSI/NIST-ITL 1-2000 standard (see Recommendation 3 above).
- **Corrective actions.** We recommend to implement an acquisition loop/recapture procedure to be carried out until satisfactory quality prints have been obtained. This procedure should contemplate alternative acquisition processes, according to the sample quality, and should include human intervention, where appropriate.

8.7.3 Identification system

RECOMMENDATION 11: Quality of identification systems

- **Quality-based processing.** In addition to the standard algorithms and tools used for fingerprint identification, we recommend the use of supplementary tools such as alternative feature extraction functions and process-specific matching algorithms.
- **Quality based fusion.** We recommend to combine different samples so as to be able to conduct composite checks. Should the revision of the SIS legislation allow this option at a later stage, it would be interesting to combine different biometric traits (e.g. multimodal biometric matching system) to improve identification results.
- **Template substitution/update.** When generating templates for an AFIS, we recommend to select best stored samples.
- **Monitoring.** We recommend to produce statistics for each type of applications, sites, devices, and operators, so as to obtain a user-scanner learning curve and propose training measures, as needed.

8.7.4 Other quality-related aspects

In addition to the previous points, other quality related aspects that should be taken into account are as follows.

RECOMMENDATION 12: Children cases

- The majority of alerts on missing persons are related to minors. We recommend that a SIS-II AFIS includes the possibility to tune the matching process towards such cases, in particular, when fingerprint data in the alert are more than two years old.

RECOMMENDATION 13: Quality check central service

- We recommend that an automated central service is offered to Member States to check fingerprint quality against the SIS-II AFIS quality metrics. A similar service exists already for the VIS with a response time of less than 30 seconds. Such a system would provide a significant additional feedback to the operator on the quality of the fingerprint dataset being acquired.

RECOMMENDATION 14: Reporting on lower quality fingerprint card

- We recommend to record when a dataset, which is proposed for enrolment or for addition in an alert, has not the quality level required for the SIS-II AFIS either in an alert or in the dataset card itself. Such a record would take place, for instance, when a ten print card is produced from a system that acquires flat prints only (e.g. the VIS).

RECOMMENDATION 15: Integrity of the database

- We recommend the use of best practices to reduce the risk of inconsistency or erroneous data, including fingerprints, recorded in the database. Efficient methods should be designed to find, mitigate, correct or prevent the occurrence of such issues. These methods are of organizational and technical nature. As an example, during a two print consultation, a cross-check should be conducted on the two fingers. In case of a match between a left index and a right index stored in the AFIS, a message should be sent to the Member States which has introduced the alert.

8.8 Consultation

Fingerprints will be also processed whenever an authority conducts a search in the SIS-II as detailed in Chapter X of the SIS-II Decision and Chapter V of the SIS-II Regulation. These consultations will take place in the course of checks at Schengen external borders or in consular posts and for checks conducted by police and border check authorities within Member States. These searches might take place in conjunction with the use of other EU large-scale IT systems such as the VIS and EURODAC. Figure 10 above within Section 8.6 describes consultations taking place in the context of law

enforcement activities and Figure 11 below summarizes the consultation cases triggered by border control.

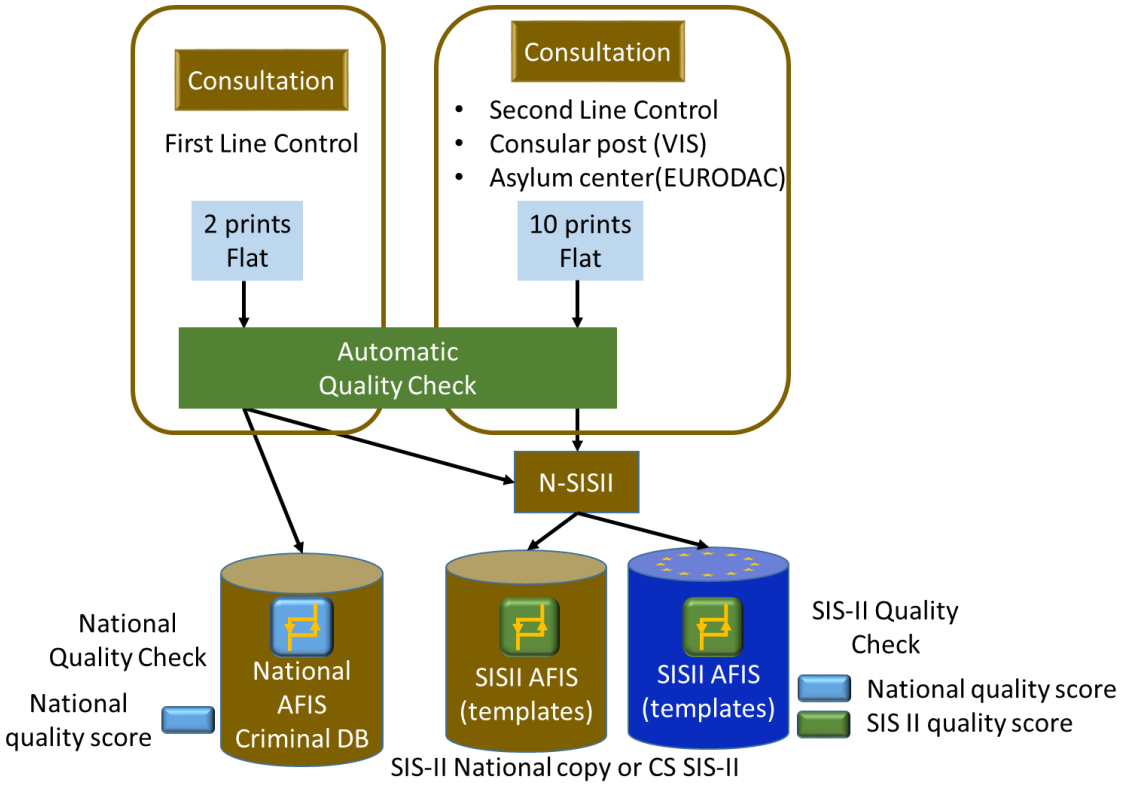

Figure 11. Border checks

Based on the use-cases identified and the expert contribution provided by Member States visited, we recommend that SIS-II AFIS should be designed so as to properly handle consultations with the following types of datasets:

RECOMMENDATION 16: Consultation

- **Enhanced resolution (1000dpi).** We recommend to give the possibility to store fingerprints at a 1000dpi resolution to those Member States that have already upgraded their scanners at that resolution.
- **Flat and rolled fingerprints.** We recommend that Member States should be allowed, for consultation only, to limit fingerprint collection only to flat prints. Member States have already implemented this option at national level since it is a faster method compared to using both flat and rolled data.
- **Two prints fast check.** We recommend to offer the possibility to carry out quick consultations. Such quick consultations are required in situations such as first line border control or on-the-spot street checks. The result of these consultations should be a hit/no hit reply which can trigger, in case of a hit, a second line control check.

Although a number of possible candidates should be proposed by default in the case of latent searches, the operator should have the opportunity to customize this number. All of these consultations will be based on different requirements regarding processing time, frequency and amount of data involved. However it can already be stated that mainly three types of time constraint will be faced according to the nature of the search.

RECOMMENDATION 17: Appropriate response times

- We recommend that the SIS-II AFIS complies with the following three response times, which are at this stage only indicative and tend to reflect the discussion which took place with Member States: (a) A very short response time (i.e. below 30 seconds) should be expected from a first line of border control check or a mobile check by a field law enforcement officer. (b) A medium response time (i.e. below five minutes) should be expected from a second line control check at the border or at a consular post (e.g. in the course of a VISA application). (c) A longer response time (i.e. up to ten minutes) could be tolerated for law enforcement consultations taking place at a police station, especially in the case of latents.

In addition, most of the Member States have implemented in their national AFIS different priority levels for the requests to be processed. As those requests are subject to a manual validation, usually centralized (such as in France and Germany), an indication of the level of urgency is necessary. If processed automatically, this level of urgency (defined and provided by the operator who entered the search) can offer the possibility of streamlining and spreading the incoming requests across the day. Accordingly, a latent request which would have been qualified as normal, should be processed within 24 hours. On the other hand the same request labelled as high priority (in relation to a terrorism event) will be processed in less than ten minutes.

RECOMMENDATION 18: Queries priority

- We recommend the definition of priority levels for processing queries in order for a SIS-II AFIS to manage better the workload of the system.

The processing time for the matching can also be reduced and optimized with the application of search tactics based on filters. It can be envisaged that the operator will link an identification query with one or several alphanumeric fields such as gender or age. In this way the search population will be reduced. On the other hand, as long as the SIS-II AFIS remains at a limited size as underlined above, such search tactics would probably not be necessary in the near future.

8.9 Performance evaluation

As described in Section 2, the performance of an AFIS is totally dependent on the data used for its evaluation. Therefore, in order to obtain an accurate picture of the performance that can be expected from the SIS-II AFIS, it is highly recommended that this assessment is conducted on the data available from the SIS-II fingerprint database itself.

RECOMMENDATION 19: Performance benchmark

- Considering that carrying out an in-depth performance evaluation is time and resource consuming, we recommend that such evaluations are planned already in the development phase of a SIS-II AFIS and are performed at the time of its rollout, as well as, every four years or every time a major update of the matching system is installed, whichever comes first.

Such periodical performance benchmarking will fulfil the following objectives:

- **Assess the actual accuracy of the matching system with its final production environ**ment. The performance of this AFIS has to be evaluated with the real data stored in the SIS-II database which are different to those used by the provider. The result obtained should not necessarily be below the performance level promised or obtained in the frame of a NIST evaluation campaign as mentioned in Section 2.
- the SIS-II fingerprint database will change over time and therefore the performance of the AFIS will not be static in time. A periodic assessment of its performance will **permit the detection of eventual drops in AFIS accuracy** which will, most likely, denote a worsening of the quality of the fingerprints being used in the system. It can also reveal improvement due

to, for example, a full adoption of live-scan devices and offer the possibility of revising some initial technical constraints.
- **adapt the different thresholds** (identification thresholds, quality thresholds) that need to be selected by the user and that have an impact on the response time of the SIS-II AFIS.
- **ensure that any update produces at least the same accuracy** (if not an improvement) with respect to the previous version.

Starting from the general context of biometric performance evaluation described in Section 2, readers interested in measuring the performance of an AFIS in an operational environment or specific application should refer to the document "Best Practices in Testing and Reporting Performance of Biometric Devices" by UKBWG (2002) and consult the standards focusing on biometric system testing: ISO/IEC 19795–1 (2006), ISO/IEC 19795–2 (2007), ISO/IEC TR 19795–3 (2007) and ISO/IEC 19795– 4 (2008). In fact, volunteer or subject selection, operational conditions, and several other issues have to be taken into consideration when a test is performed in a laboratory or in the field. From a general point of view, practitioners should try to avoid some common mistakes in evaluating the performance of their matching algorithms such as:

- avoid using the same dataset for training, validating and testing an algorithm.
- do not compute performance on a very small dataset and, in particular, abstain from claiming that a system has a very low error rate when the errors have been measured over a small dataset; if possible, report the statistical significance of the results (e.g. confidence intervals).
- avoid "cleaning" the database by removing samples that are either "rejected" or misclassified by the system; in principle, by iteratively removing the unwanted samples, one could reach any desired level of accuracy.
- do not conclude that the accuracy of a system is better than that of a competing system when they have been evaluated using different datasets.
- do not hide the weak points of an algorithm but document its failures.

As underlined above, such a benchmark exercise will be relevant only if it is conducted on the datasets actually stored in SIS-II. This task will require access to the data and their corresponding ground-truth meta-data needed for the evaluation and therefore an active involvement of the Member States together with eu-LISA must be foreseen.

9 Beyond the SIS-II regulatory framework

In April 2015, the European Commission adopted a Communication on "The European Agenda on Security" C(2015) 185 final[23] setting out how the EU can bring added value to supporting the Member States in ensuring security. Among other actions aimed at strengthening information exchange, the Commission announced that the SIS will be evaluated in 2015-2016 to assess whether new operational needs require legislative changes, such as introducing additional categories to trigger alerts. Considering new technological initiatives conducted by the countries visited in the course of the JRC study, we suggest in this section a series of possible new operational tools and functionalities which might be interesting to consider in the context of the review of the SIS-II regulatory framework.

It has to be underlined that, at this stage, these suggestions are of a prospective nature and will require additional targeted analysis in order to be possibly included in a revision of the SIS legislative framework.

9.1 Additional biometric modalities

9.1.1 Palm recognition

As numerous Member States are currently using the NIST container and standard for uploading fingerprint images in the SIS-II, it is quite probable that palm prints might have already been introduced as they are usually part of this container.

All the Member States visited have databases containing palm prints and process them with their respective AFIS in the course of investigating crime.

An introduction of palm prints in SIS-II would imply a modification of the legal framework and an adaptation of the envisaged AFIS which would need to cope with such prints although no fundamental technical differences exist. They can be processed using the same matching characteristics. It should be underlined that in the Prüm Decision, the term "dactyloscopic data" is used and covers both palm print and fingerprints.

If introduced in SIS-II palm prints will be used exclusively in the context of crime scenes from which latent prints might be collected and compared with those stored in the SIS-II AFIS.

9.1.2 Face recognition system

Some Member States have already started to test face recognition solutions (e.g. The Netherlands, Spain, Germany). As confirmed by all of them, such functionality would constitute a solid improvement, as in some cases this might be the only available data. It has to be underlined that according to Article 22(a) faces are already added to alerts and stored in the SIS-II (around 40 000 at the end of 2014).

Although not as accurate as ten print against ten print matching systems, face recognition has made significant progress. The quality of the image and therefore the performance of the matching system are heavily dependent on the conditions of capture and, in the case of SIS-II, it can be expected that such conditions will be optimised as the uploaded images are at least of a frontal mugshot produced in a completely controlled environment (light exposure, angle, resolution, background etc.)

The introduction of face recognition functionality in the SIS-II would require modification of Article 22(c) and the rollout of an appropriate dedicated matching functionality adapted to this modality.

[23] http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

However, it should be underlined that a special quality check is already required (Article 22(a)) whenever a face image is uploaded to an alert, the nature of this quality check remains to be defined.

9.1.3 Latent database

All national AFIS visited by the JRC contain in addition to the ten prints sets, a database of latent fingerprints linked with unsolved crime cases. As described in Technical cases 4 and 5 of Section 4.1, this latent database is typically used by Member States as a second step process when the other uses cases (ten prints vs ten prints) didn't produce any hit. Requests applied to latent databases require more processing time than the usual ten prints against ten prints (all orientations of the print have to be envisaged and all combinations tested).

Today, the SIS-II legal framework does not provide a category of alert for which those latent fingerprints could be stored in the system.

9.2 Future of SIS-II: Further Experimentation

The JRC has already conducted some biometric experiments related to the quality of children's fingerprints which are described together with their results and conclusions in [JRC2013]. Such experiments were possible thanks to the collaboration of the Portuguese Authorities which provided a gross sample of their national fingerprint database for electronic passports. This collaboration was successfully renewed in June 2015 for two years with an even larger set of fingerprints (slightly more than 200 000) which also includes adults and the elderly. This sample database will enable the JRC to conduct some quality-related experiments that could be of relevance for the future of SIS-II and in particular its AFIS.

According to the general fingerprint quality context presented in Section 3, some of the tasks that could be performed by the EU research community in the future regarding the development of the SIS-II would include:

- generation of a reference dataset for quality evaluation (this evaluation will be however limited to flat prints),
- comparison between NFIQ with NFIQ2 and predicting its relevance for SIS-II AFIS performance,
- comparison of NFIQ/NFIQ2 with other proprietary quality metrics,
- use of the NFIQ2 modular design that allows for self-training the neural network classifier on various categories of data and develop a dedicated version for children (to be used with alerts on missing persons),
- fingerprint quality comparison among significant age groups: children, adults, elderly.

JRC will launch, in 2016, an AFIS performance competition which can be adapted to the SIS-II context with the active support of the Member States and provide useful results analysis for a future SIS-II AFIS deployment.

10 Conclusion

For more than 35 years (starting with the FBI NBS M40 algorithm brought into operation in the 1960's) AFIS functionality has been intrinsically linked with databases supporting law enforcement and border management activities. According to its general purpose, SIS-II constitutes one of those databases and therefore SIS-II alerts related to persons will not deliver their full capacity and usefulness without the support of an Automatic Fingerprint Identification System.

AFIS technology has reached sufficient levels of readiness and availability for its integration into SIS-II, provided that all recommendations listed in the present report are implemented and respected during the rollout and utilization of the new functionality.

The rollout of AFIS functionality should be preceded with the selection of the most appropriate special quality check tools (as required by Article 22(a)) and with the production of detailed statistics on consultations related to persons as carried out currently in SIS-II.

References

[Alonso2010] F. Alonso-Fernandez, J. Fierrez, D. Ramos and J. Gonzalez-Rodriguez, "Quality-Based Conditional Processing in Multi-Biometrics: application to Sensor Interoperability", *IEEE Transactions on Systems, Man and Cybernetics Part A*, Vol. 40, n. 6, pp. 1168-1179, 2010.

[Alonso2012] F. Alonso-Fernandez, J. Fierrez and J. Ortega-Garcia, "Quality Measures in Biometric Systems", IEEE Security & Privacy, Vol. 10, n. 9, pp. 52-62, 2012.

[Cappelli2006] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman and A. K. Jain, "Performance Evaluation of Fingerprint Verification Systems," IEEE. Trans. on Pattern Analysis and Machine Intelligence, vol. 28, pp. 3-18, 2006.

[Cappelli2015] R. Cappelli, M. Ferrara and D. Maltoni, "Large-scale fingerprint identification on GPU", Information Sciences, Vol. 306, pp. 1-20, 2015.

[Champod2004] C. Champod, C. J. Lennard, P. Margot and M. Stoilovic, "Fingerprints and other ridge skin impressions", CRC Press (International Forensic Science and Investigation Series), 2004.[FBI2013] J. Carlyle, "Best practices and time utilization in searching local, state and federal AFIS", FBI presentation, 2013.

[Galbally2014] J. Galbally and S. Marcel and J. Fierrez, "Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition", *IEEE Trans. On Image Processing*, Vol. 23, pp. 710-724, 2014.

[Grother2007] P. Grother and E. Tabassi, "Performance of Biometric Quality Measures," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 531–543, 2007.

[ISO2011] ISO/IEC 19794-2. Information technology-Biometric data interchange formats-Part 2: Finger minutia data

[Jarosz2005] H. Jarosz, J. C. Fondeur, X. Dupre, "Large-Scale Identification System Design", Biometric Systems, Springer, 2005.

[JRC2013] JRC report on Children Fingerprints, http://publications.jrc.ec.europa.eu/repository/handle/JRC85145

[Langenburg2012] G. Langenburg, C. Champod and T. Genessay. "Informing the judgments of fingerprint analysts using quality metric and statistical assessment tools", Forensic Science International, Vol. 219, pp. 183-198, 2012.

[Maltoni2009] Davide Maltoni, Dario Maio, Anil K. Jain and S. Prabhakar (eds.), "Handbook of Fingerprint Recognition", Springer, 2009.

[NIST2004] C. Wilson, R. A. Hicklin *et al*, "Fingerprint Vendor Technology Evaluation 2003: Summary of results and analysis report", NISTIR 7123, 2004.

[NIST2004b] E. Tabassi, C. L. Wilson and C. I. Watson, "Fingerprint Image Quality", NISTIR 7151, 2004.

[NIST2005] C. Watson, C. Wilson, K. Marshall, M. Indovina and R. Snelick, "Studies of one-to-one fingerprint matching with vendor SDK matchers", NISTIR 7221, 2005.

[NIST2006] V. N. Dvornychenko and M. D. Garris, "Summary of NIST latent fingerprint testing workshop", NISTIR 7377, 2006.

[NIST2006b] P. Grother, M. McCabe *et al*, "MINEX. Performance and interoperability of the INCITS 378 fingerprint template", NISTIR 7296, 2006.

[NIST2009] M. Indovina, V. Dvornychenko *et al*, “ELFT Phase II – An evaluation of automated latent fingerprint identification technologies”, NISTIR 7577, 2009.

[NIST2011] M. Indova, R. A. Hicklin and G. I. Kiebuzinski, “ELFT-EFS. Evaluation of Latent Fingerprint Technologies: Extended Feature Sets”, NISTIR 7775, 2011.

[NIST2011b] P. Grother, W. Salamon, C. Watson, M. Indovina and P. Flanagan, “MINEX-II. Performance of fingerprint Match-On-Card algorithms. Phase IV Report”, NISTIR 7477, 2011.

[NIST2013] ANSI/NIST-ITL 1-2011. Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information, Update 2013.

[NIST2014] C. Watson, G. Fiumara *et al*, “Fingerprint Vendor Technology Evaluation”, NISTIR 8034, 2014.

[Tabassi2007] Elham Tabassi, “The last 1% - Biometric quality assessment for error suppression”, Presentation at the Biometric Consortium (BC), 2007.

[Ulery2014] B. Ulery, R. A. Hicklin, M. A. Roberts and J. Buscaglia, “Measuring what latent fingerprint examiners consider sufficient information for individualization determinations”, *PLoS ONE*, Vol. 9, e110179, 2014.

[Yoon2013] S. Yoon, E. K. Liu, A. K. Jain, “LFIQ: Latent Fingerprint Image Quality”, in *Proc. Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2013.

Annexes

This page is intentionally left blank.

Annex 1: Main definitions and technical concepts of an AFIS

This annex contains a brief introduction to the main definitions and technical concepts of Automatic Fingerprint Identification Systems. All relevant concepts are highlighted throughout the text in **underlined bold** characters.

All the terms introduced here are used and referenced in the main sections of the report, therefore, it is highly recommended for those readers who are not familiar with biometric technology to carefully read this annex before proceeding to the rest of the document.

The annex is divided in three main sections: 1) a general introduction to biometric technology; 2) a summary of the methodologies and metrics used for the performance assessment of identification systems; 3) an introduction to AFIS in the light of the previous two sections.

A1.1. Introduction to biometrics

A biometric system is essentially a pattern recognition system that makes use of biometric traits to recognize individuals. The objective is to establish an identity based on "*who you are or what you produce*", rather than by "*what you possess*" or "*what you know*". This new paradigm not only provides enhanced security but also avoids, in authentication applications, the need to remember multiple passwords and maintain multiple authentication tokens. "Who you are" refers to physiological characteristics such as fingerprints, iris, or face. "What you produce" refers to behavioural patterns which entail a learning process and that characterize your identity such as the written signature.

As shown in Figure 1, biometric systems use a specific device known as a **sensor** (also referred to in some cases as a scanner) to acquire the physical biometric trait and generate a digitized version known as a **biometric sample**, named as *B* in Figure 12 (e.g. in the case of fingerprints the biometric sample *B* is the fingerprint image). Then, in a subsequent step, the biometric sample is processed in order to extract the most discriminating features (feature extraction module). These features conform to what is known as **biometric template**, named as *T* in Figure 1. Templates are stored in the system database together with an associated identity I through the **enrolment process**. Therefore, after enrolment, a biometric database typically contains *N* templates T_n and their respective I_n identities, with *n*=1,..,*N*.

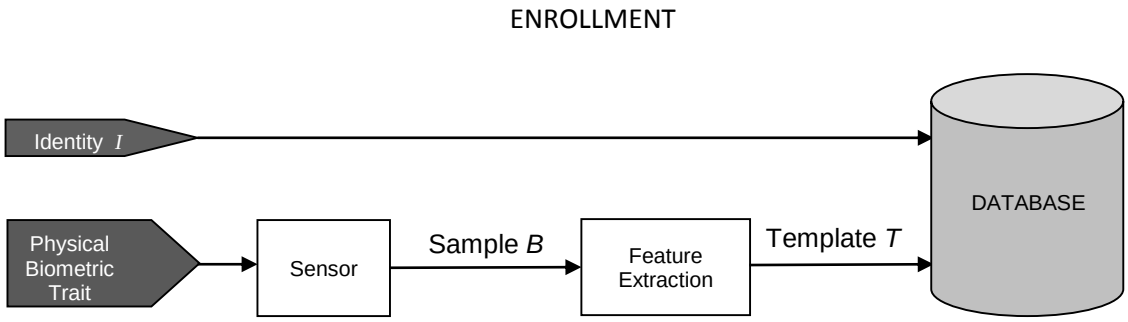

Figure 12 Flowchart describing the enrolment process in a typical biometric system.

Once the users have been enrolled to the system, the recognition process can be performed in two modes:

- **IDENTIFICATION** (Figure 2, top). In this mode, the question posed to the system is: is this person in the database? The answer might be "No" (the person is unknown to the system), or any of the *N* registered identities in the database. In order to give the answer, the system compares the test template *T* to each of the T_n templates stored in the database. This

comparison process is known as **matching process**. For each pair (T, T_n), the matching module outputs a value referred to as **similarity score** that reflects the level of similarity between the two compared templates.

Therefore, identification is a search operation in which a template T is used to determine if it corresponds to any of the I_n identities stored in the database. For this reason identification is known as a "1 to N" recognition process (also "one-to-many"), as one template is matched against N.

In order to determine if the test template T corresponds to any of the identities enrolled in the database, a **decision threshold** δ is set. If one or more of the N matching scores s_n exceed the threshold, the system typically returns a ranked list with the M most likely identities that correspond to the searched person (i.e. those that generated the M highest scores above the threshold). If none of the N scores s_n is higher than this threshold, the searched identity is considered to *not* be stored in the database (the ranked list is empty, that is, it contains M=0 identities).

When the maximum size of the ranked list is set to M=1, it is commonly known as a **hit** or **no-hit** system, that is, the system will only output one identity (expected to be the correct one) or none. In most identification systems, at a later stage, a human expert manually checks the results and decides whether the subject is or is not within the reduced group of M ranked identities. Typical identification applications include Automatic Fingerprint Identification Systems (AFIS).

- **VERIFICATION** (Figure 13, bottom). In this case, what we want to know is if a person is really who she claims to be: is this person truly John Doe? This way, under the verification mode, the system performs a "1 to 1" matching process where the test biometric template T is compared to the enrolled template T_I associated with the claimed identity I. This matching process produces a single score s which is compared to a decision threshold δ in order to determine if the subject is a client (the identity claim is accepted as the score is higher than the threshold), or an impostor (the identity claim is rejected as the score is lower than the threshold).
  Typical verification applications include network logon, ATMs, physical access control, credit-card purchases etc.

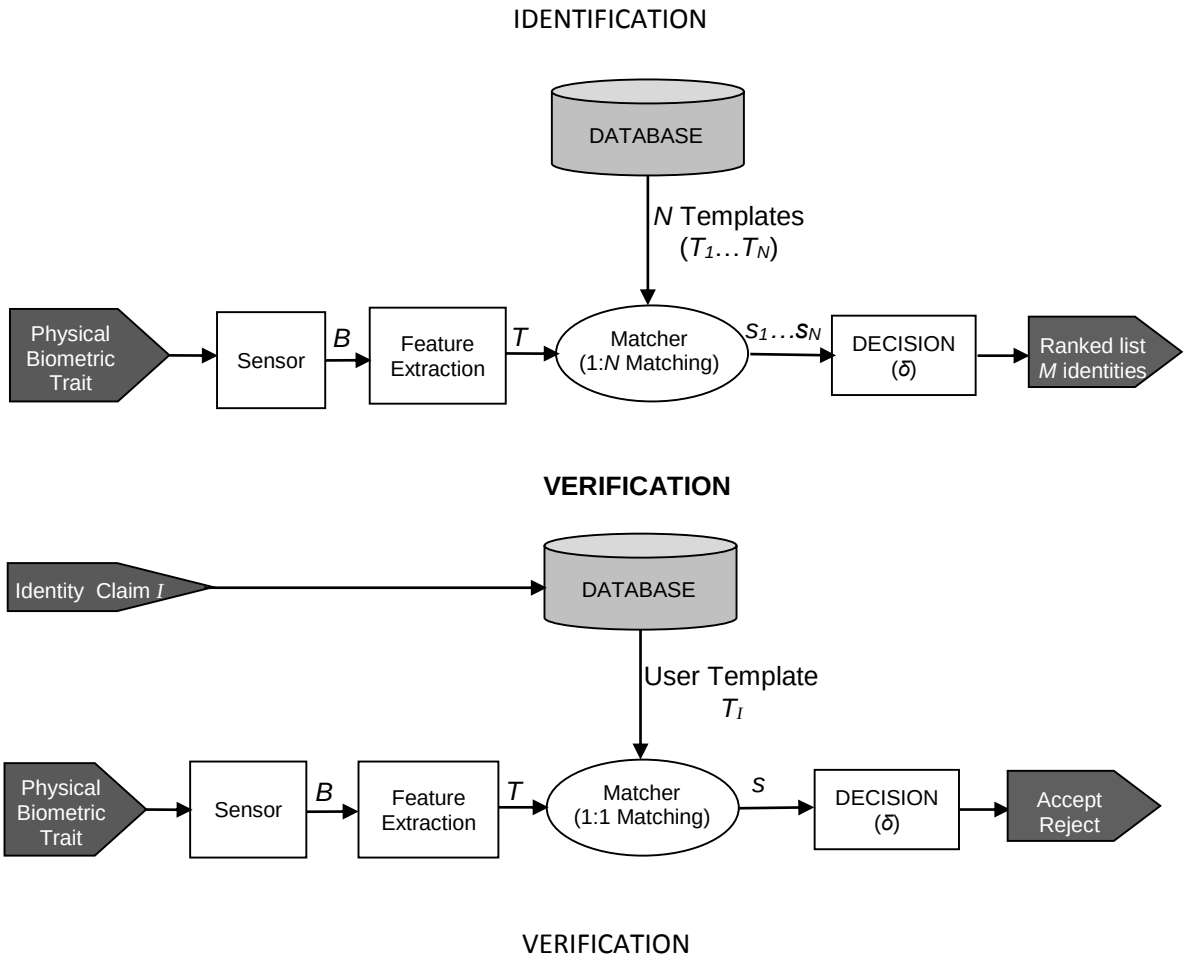

Figure 13 Flowchart describing the identification (top) and verification (bottom) recognition processes in a typical biometric system.

A1.2. Accuracy evaluation of biometric identification systems

As described in the previous section, in biometrics, an identification task may be defined as a problem in which a biometric test sample has to be assigned to one of the identities corresponding to the enrolled biometric templates in a database. Therefore, the question being addressed is: Within this given database, who does this sample belong to?

Two general identification scenarios are possible: open set and closed set.

- **Closed-set**: in the closed-set scenario it is known beforehand that the test sample positively belongs to one of the identities included in the dataset. Therefore, the answer to the question raised above is "John Doe" (i.e. the searched identity within the database). In this scenario, identification systems give an output as a ranked list with the first *M* the most probable identity within the database for the test sample, where *M*>0, that is, the output cannot be an empty list.

In the case of a closed set scenario, identification systems can make only one type of error: A search using a biometric sample of an enrolled individual returns an *incorrect* identity. This is considered a miss, because it misses the correct identity.

- **Open-set**: the open-set scenario represents a more challenging problem than the closed-set case both from a technical and an evaluation point of view, as the test sample may or may not belong to one of the identities included in the dataset. Hence, there are two possible answers to the question raised above: "nobody" (i.e. in the case that the searched sample is not present in the database), or "John Doe" (i.e. in the case where the test sample does belong to one of the identities in the database). Therefore, in this scenario, the ranked list with *M* candidates can be empty, meaning that the searched subject is not in the database, i.e. $M \geq 0$.

In the open-set scenario, identification systems can make two types of error:

1) A search performed with a biometric sample of an individual not enrolled in the biometric database (a non-mated search) returns the identity of one or more enrolled subjects. This is considered a false alarm, because it returns a false identity.

2) (Same as in the closed-set scenario). A search using a biometric sample of an enrolled individual (mated search) returns an *incorrect* identity. This is considered a miss, because it misses the correct identity.

Most Automatic Fingerprint Identification Systems (AFIS) used in the fight against criminal activities work under the open-set scenario.

The open-set scenario comprises the type of error that can be committed in the closed-set scenario, therefore, we will define below the most common metrics used to evaluate the accuracy of open- set identification systems (as these can also be used for the closed-set).

Accuracy assessment of identification systems is not a trivial task and different metrics have been defined in the literature with this objective. In the following we will present the most commonly used and accepted metrics as defined in the 2012 NIST Fingerprint Vendor Technology Evaluation, see Section 2.1 and reference [NIST2014].

False Positive Identification Rate (FPIR): is the fraction of the non-mated searches (i.e. searches of an identity that is not in the database), where one or more enrolled identities are returned at or above threshold δ. FPIR is a function of: the size of the enrolment set (N), length of the candidate list (M) and score threshold (δ). In the general case, this can be summarized as:

$$\mathrm{FPIR}(N, M, \delta) = \frac{\text{Number of searches with any non} - \text{mates returned above threshold } \delta \text{ on candidate list of length } M}{\text{Number of non} - \text{mated searches conducted}}$$

False Negative Identification Rate (FNIR): is the fraction of the mated searches (i.e. searches of an identity that does exist in the database), where the enrolled mate is outside the top M rank or that the comparison score is below threshold δ. FNIR is a function of: the size of the enrolment set (N), length of the candidate list (M), score threshold (δ) and the number of top candidates being considered (R). In the general case this can be summarized as:

$$\mathrm{FNIR}(N, M, \delta, R) = \frac{\text{Number of mates ouside top } R \text{ ranks or below threshold } \delta \text{ on candidate list of length } M}{\text{Number of mated searches conducted}}$$

Note that FNIR computation does not care about the cause of a miss: failure to correctly identify a sample (e.g. due to poor quality), failure to extract a template, failure to generate a comparison score and software crashes are all dealt in the same way.

It should also be highlighted that, in the most usual case, both the length of the candidate list and the number of top candidates being considered take the same value, that is, M=R.

The terms “hit rate,” “reliability,” and “sensitivity” that have been mentioned in some literature on Automatic Fingerprint Identification Systems (AFIS) are just the complement of FNIR, computed as 1-FNIR.

Detection Error Trade-off (DET) plots: DET characteristic curves are the primary accuracy metric for offline testing of biometric recognition algorithms. Each point on a DET curve exhibits the False Positive Identification Rate (FPIR) and False Negative Identification Rate (FNIR) associated with a certain threshold value. The DET curve spans the entire range of possible threshold values, which is normally the range of the comparison scores. To reveal the dependence of FNIR and FPIR at a fixed threshold the DET curves are connected at points where FNIRs and FPIRs are observed at the same threshold values.

In a typical DET curve, FPIR is plotted on the x-axis and FNIR is plotted on the y-axis, giving uniform treatment to both types of error. In general, both axes use a logarithmic scale which spreads out the plot and helps to distinguish between different well-performing systems. A different DET curve is computed for every pair of values (M, R). As mentioned before, in order to simplify, it is very commonly assumed that M=R.

An example of DET curves for different systems competing in FpVTE 2012 [NIST2014] is given in Figure 14. A system presents better accuracy the closer its DET curve is to the bottom left corner of the plot. In the particular case of Figure 3 the best system would be the one represented with the red dotted line.

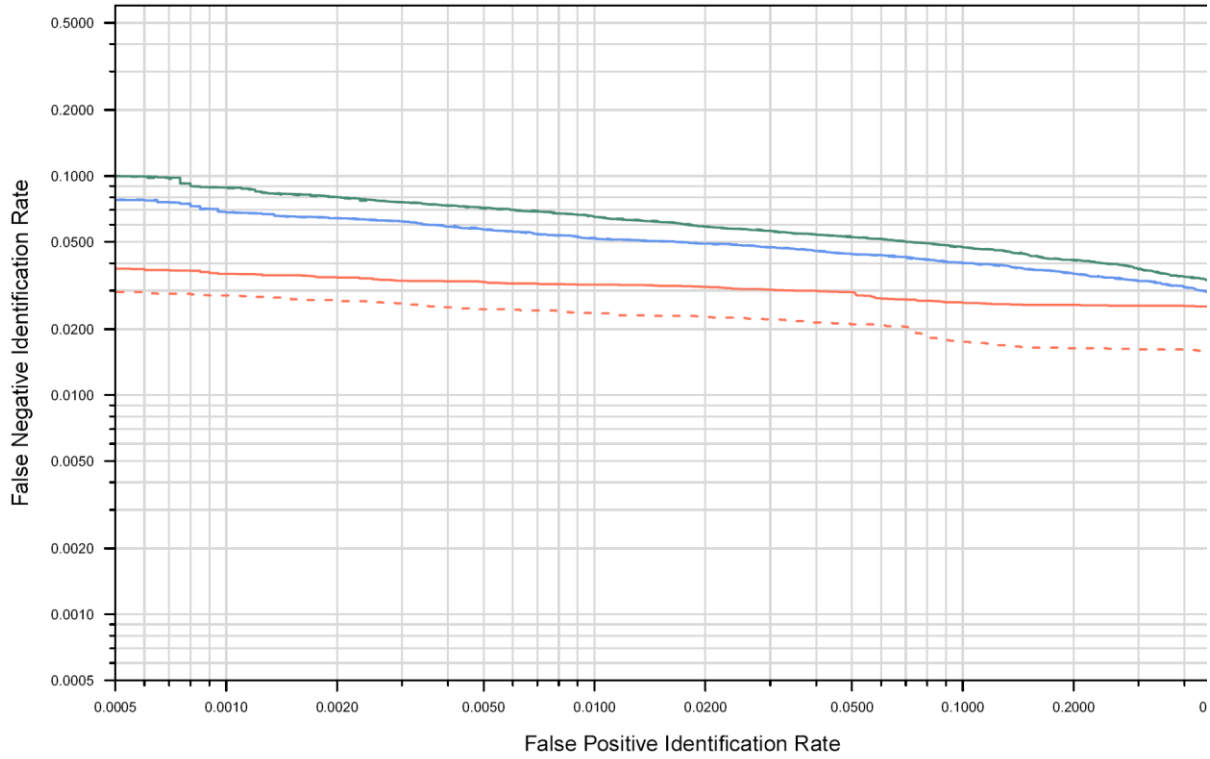

Figure 14 Detection Error Trade-off (DET) curves corresponding to four systems participating in the NIST FpVTE 2012 competition. A better system is one that is closest to the bottom left corner. Figure extracted from [NIST2014].

Cumulative Match Characteristic (CMC): this is another widely used accuracy metric which corresponds to the fraction of the mated searches where the enrolled mate is at rank *R* or better, regardless of its comparison score. An example of CMC curves is shown in Figure 15. CMC is a special case of FNIR, or more precisely, the hit rate when the constraint on threshold is removed, that is:

$$\mathrm{CMC}(N, M, R) = 1 - \mathrm{FNIR}(N, M, \delta = 0, R)$$

Rank-one hit rate, CMC (*N*,*L*,*R* = 1), is the most common accuracy metric reported in academic and AFIS-related literature. While the use of CMC is very widespread, it presents two major issues: 1) it makes strong or weak hits indistinguishable by ignoring similarity scores, and 2) it does not report on false alarms (i.e. a sample of an individual not enrolled in the database is mated to an enrolled identity), therefore, on its own, it should only be used to present results of systems working on closed-sets.

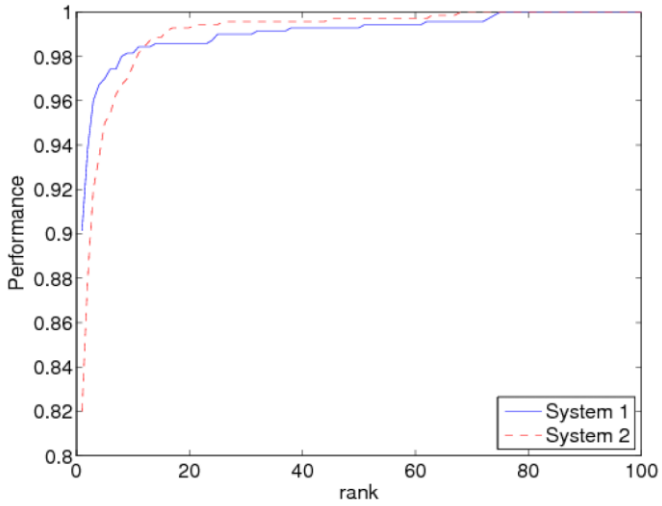

Figure 15 Closed-set identification accuracy of two systems reported on the same database using CMC.

A better system is one that is closest to the top left corner of CMC. In this example, system 1 has a higher identification rate up to rank 12. Beyond this rank, system 2 has a better identification rate. Hence, in this case, neither of the two systems being compared is systematically better than the other across all ranks.

Failure to Extract a Template: Failure to extract a template is the fraction of images for which a template is not generated. Template generation can fail for the enrolment sample or the search sample. Although this is a metric that can be useful on its own and from which interesting conclusions may be drawn, in general it is included as a miss in the computation of FNIR.

Failure to Match a Template: In some cases, recognition algorithms fail to execute one-to-many searches to produce comparison scores. The result is that a valid candidate list is not produced. Such failures might be voluntary (e.g. refusal to process a poor quality image) or involuntary (e.g. software crashes). Either way, it is an undesirable behaviour, and should be included in the computation of recognition errors, particularly to allow for fair comparison of submissions. In general, such failure cases are computed as a miss and included in the FNIR. As in the case of the failure to extract, this metric can also be reported on its own as an informative parameter regarding the accuracy of a system.

A1.3. Introduction to AFIS

This report is focused on the analysis of Automatic Fingerprint Identification Systems (AFIS) and their use in a large scale law-enforcement scenario.

An AFIS is an identification biometric system based on fingerprints. In the case of law enforcement scenarios, such systems work almost in all cases in the open-set mode. Therefore, all the concepts introduced above for open-set biometric identification systems are applicable to the case of an AFIS. The distinctive features of an AFIS with respect to other biometric identification systems come from the fact that fingerprints are used as the base for recognition. As such, in this section, some important concepts related to fingerprints which directly impact AFIS technology are introduced.

The section is not intended as a detailed analysis and description of fingerprint recognition (this would fall out of the scope of the report), but rather as a tool of quick reference for the reader to understand

and form a general view of the most important fingerprint-related terms that are used throughout the main sections of the document. For exhaustive reading on fingerprint recognition systems we refer the reader to [Maltoni2009].

A1.3.1. General fingerprint-related concepts

Terms will be introduced following the general flow-charts showed in Figures 1 and 2, that is: physical biometric trait, biometric sensor, biometric sample and biometric template.

- **Fingertip**: the physical biometric trait used by AFIS to identify individuals is the fingertip of human fingers and thumb. The fingertip's epidermis presents a unique pattern of 3D formations known as **ridges** and **valleys**.

- **Fingerprint scanner**: multiple types of biometric scanner exist at present (see below the definition of inked and live-scanned fingerprints for further details). Although different technologies and methods are used, essentially all of them translate the physical 3D skin pattern of the fingertip into a 2D digital image. There are multi-finger and single-finger scanning devices depending on whether they are capable or not of acquiring more than one fingerprint at the same time.

- **Fingerprint**: this is the biometric sample used by AFIS in the recognition process. It corresponds to the 2D image produced by the fingerprint sensor. In general this is a grey- scale image where ridges and valleys are visible usually in dark shades (ridges) and light shades (valleys). See Figure 16 for a flowchart showing a fingertip and its corresponding fingerprint acquired with an optical scanner.

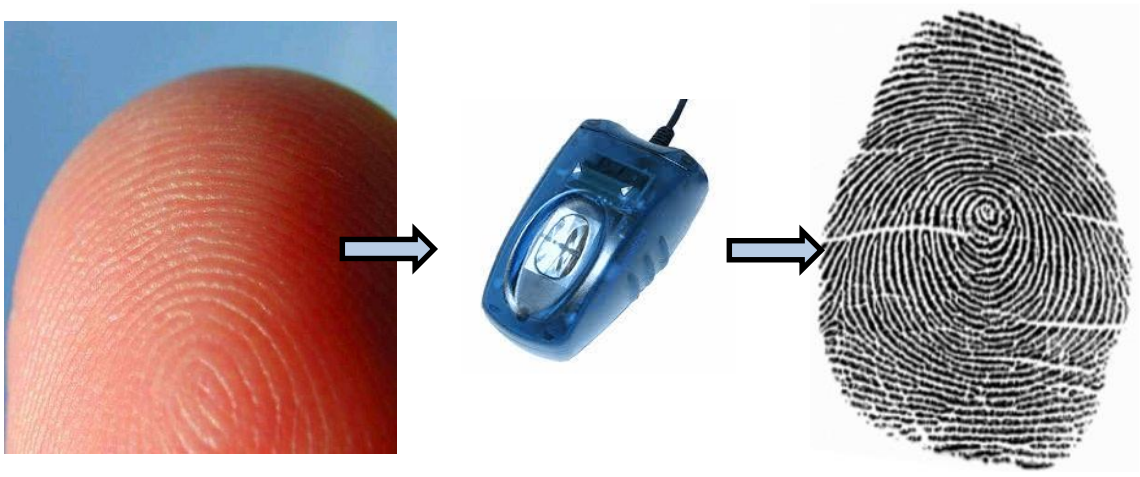

Figure 16 Fingertip (left), fingerprint scanner (middle) and fingerprint image (right).

It should be highlighted that, although strictly speaking a fingerprint is a 2D impression of the fingertip 3D pattern, in practice in the literature, the term is largely used to also refer to the physical 3D skin pattern.

- **Minutiae points**: although nowadays fingerprint templates contain a great diversity of information extracted from the fingerprint, the vast majority of fingerprint recognition algorithms use the minutiae points as the most distinctive features. The most common minutiae points are defined as the points where a ridge ends or where a ridge presents a

bifurcation (see Figure 17). The usual information that is stored in the fingerprint template for each minutiae point is: its coordinate within the image, its angle, its type and a reliability indicator. Although a standard ISO template exists to encode minutia data [ISO2011], most vendors have their own proprietary template format where additional information is stored.

As defined in the previous sections, once the fingerprint templates have been generated, AFIS compare them to produce similarity scores and take a decision on the test sample. Such matching processes (as well as all the previous terms) are thoroughly discussed in [Maltoni2009].

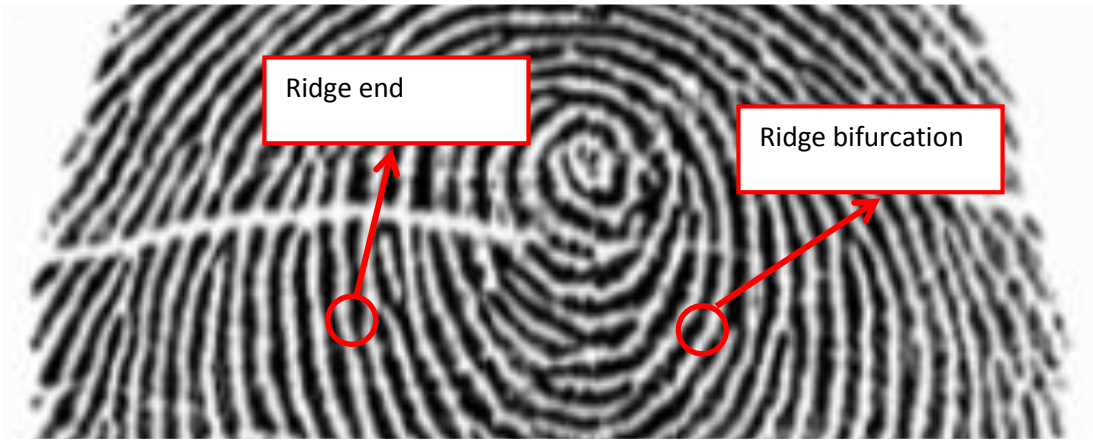

Figure 17 Examples of two minutiae points: a ridge end and a ridge bifurcation

A1.3.2. Types of fingerprint data

Although different categorizations of fingerprint data are possible [Champod2004], in this section we will focus on those types that typically have to be dealt with by AFIS. All the terms introduced in this section are systematically used throughout the report. A general diagram with the classification followed is shown in Figure 18. In the following, we will define the different terms that appear in the diagram.

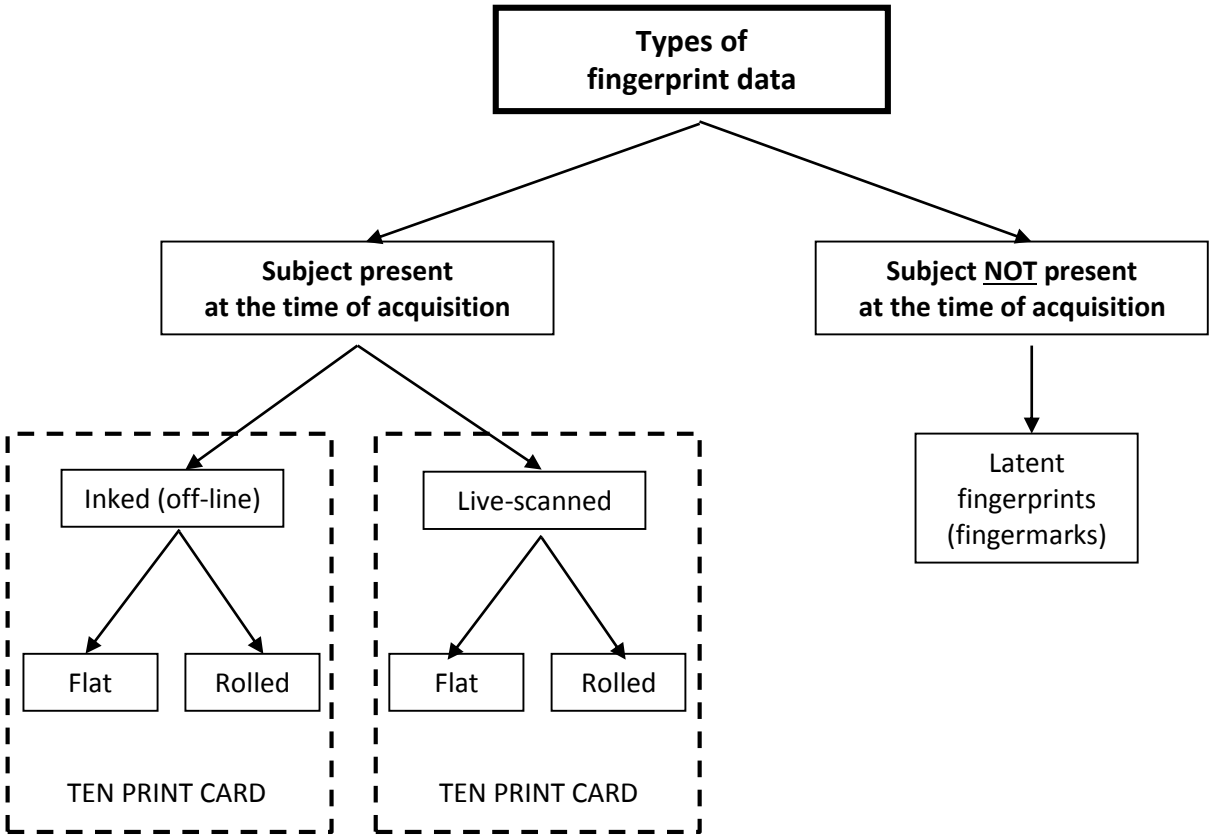

Figure 18 . Diagram with the most relevant types of fingerprint data mentioned in the report.

Fingerprints that are acquired directly from the subject may be classified according to:

- Type of acquisition sensor: inked / live-scanned.

Inked fingerprints: also known as off-line fingerprints. They are typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on paper. The inked impression is then digitized by scanning the paper using an optical scanner or a high-quality video camera (the most common resolution for the scanner/camera is 500dpi). The ink-technique often produces images that include regions with missing fingerprint information due to excessive or insufficient ink on the finger or excessive or insufficient finger pressure.

Live-scanned fingerprints: A live-scan image, on the other hand, is acquired by scanning the tip of the finger directly, using a specific device that is capable of digitizing the fingerprint on contact. There are a number of live-scan sensing mechanisms (e.g. optical, capacitive, thermal, pressure-based, ultrasound etc.) that can be used to detect the ridges and valleys present on the fingertip. The most important part of a live-scan fingerprint scanner is the sensor (or sensing element), which is the component where the fingerprint image is formed. In many cases, in the literature, both terms, scanner and sensor, are used interchangeably to denote the whole scanning device. Such devices present different resolutions, the most typical being 500dpi and 1000dpi.

The use of ink-techniques is gradually being replaced as live-scan acquisition technology is becoming more affordable. As a result, the databases that have been built by law enforcement agencies over a long period of time contain fingerprint images acquired by both off-line as well as live-scan scanners. The AFIS fingerprint recognition algorithms are expected to interoperate on these different types of

image. In other words, an image acquired using an off-line scanner needs to be matched to an image acquired using live-scan scanners with the minimum loss of accuracy possible.

Figure 19 shows some live-scan images acquired with different types of commercial live-scan devices and an off-line fingerprint image acquired with the ink technique.

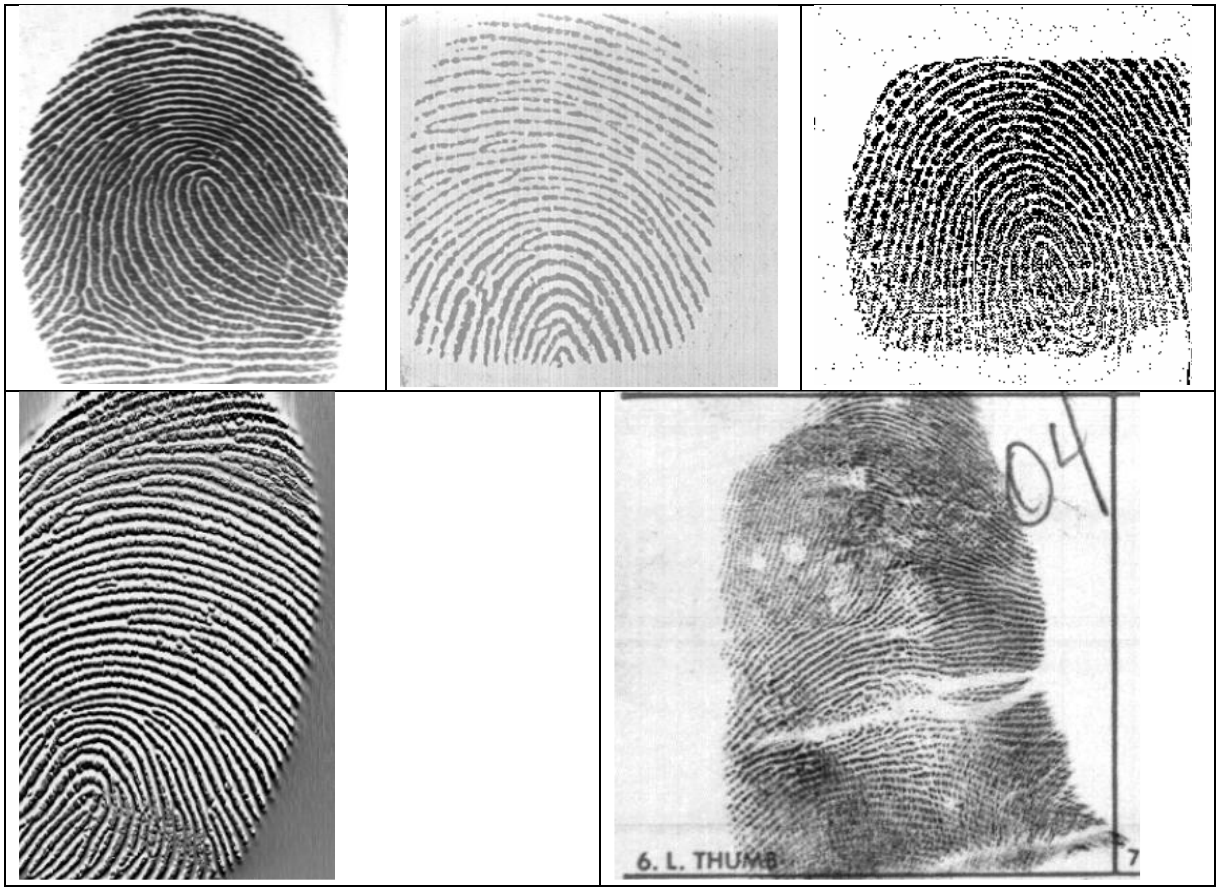

Figure 19 Examples of fingerprint images from (left to right and top to bottom): live-scan optical scanner, live-scan capacitive scanner, live-scan piezoelectric scanner, live-scan thermal scanner, inked impression.

- Acquisition procedure: flat /rolled

Flat fingerprints: these impressions (also called dab, slapped or plain) are obtained when the user simply places his/her fingertip on the acquisition surface (i.e. scanner or paper) and applies some pressure without moving it (see Figure 20 left).

Rolled fingerprints: to obtain these impressions the user is required to roll a finger "nail-to-nail" on the scanner/paper, thus producing an unwrapped representation of the whole fingerprint pattern which carries more information than a flat impression (see Figure 20 right). It is often necessary for a trained fingerprint acquisition expert to assist the user in rolling his/her finger on the sensor/paper.

The reader should be aware that, as shown in the diagram in Figure 18, the previous two classifications are not exclusive. That is, flat fingerprints can be both inked and live-scanned (depending on the acquisition device), the same way that rolled fingerprints can also be inked or live-scanned.

Figure 20. The same finger acquired as a flat fingerprint (left) and as a rolled fingerprint (right). On the rolled impression, the portion corresponding to the flat fingerprint is highlighted in lighter grey. As may be observed, rolled fingerprints provide a larg

In AFIS the previous fingerprint data is stored in **ten print cards**. A ten print card is a container, either in paper (for inked fingerprints) or a digital file (for live-scanned fingerprints) that comprises the fingerprints of all eight fingers and two thumbs of an individual, both flat and rolled. In the case of paper ten print cards, they are digitized using an optical scanner or a high definition camera (similar to what is done with single inked fingerprints). An example of a typical ten print card is shown in Figure 21.

Usually, as can be observed in Figure 21, in ten print cards, the flat fingerprints of the four fingers of each hand are acquired at the same time as "slaps" which may include also imprints of the second and third limb. Ten print cards may also include the two palm prints.

In cases in which more than one ten print card of the same individual is available, some AFIS build a **composite ten print card** that contains the best quality individual fingerprints coming from the different ten print cards available (i.e. the best quality: left index flat, left index rolled, right index flat, right index rolled, middle finger flat etc.)

As mentioned previously, ten print cards were initially enrolled as paper-and-ink records that were digitized in a successive step. However, currently these hard-copy cards are progressively being replaced by their electronic equivalent by directly capturing the fingerprints with live-scan scanners. In most cases AFIS store the digital ten print cards in electronic containers or files (also called cards) following the standard introduced by the US National Institute of Standards and Technology (NIST), [NIST2013]. Alternatively, fingerprints may be transmitted in some loss-less image format (e.g. JPEG2000) where the link to other images and additional meta-data has to be established in a non-standardized way.

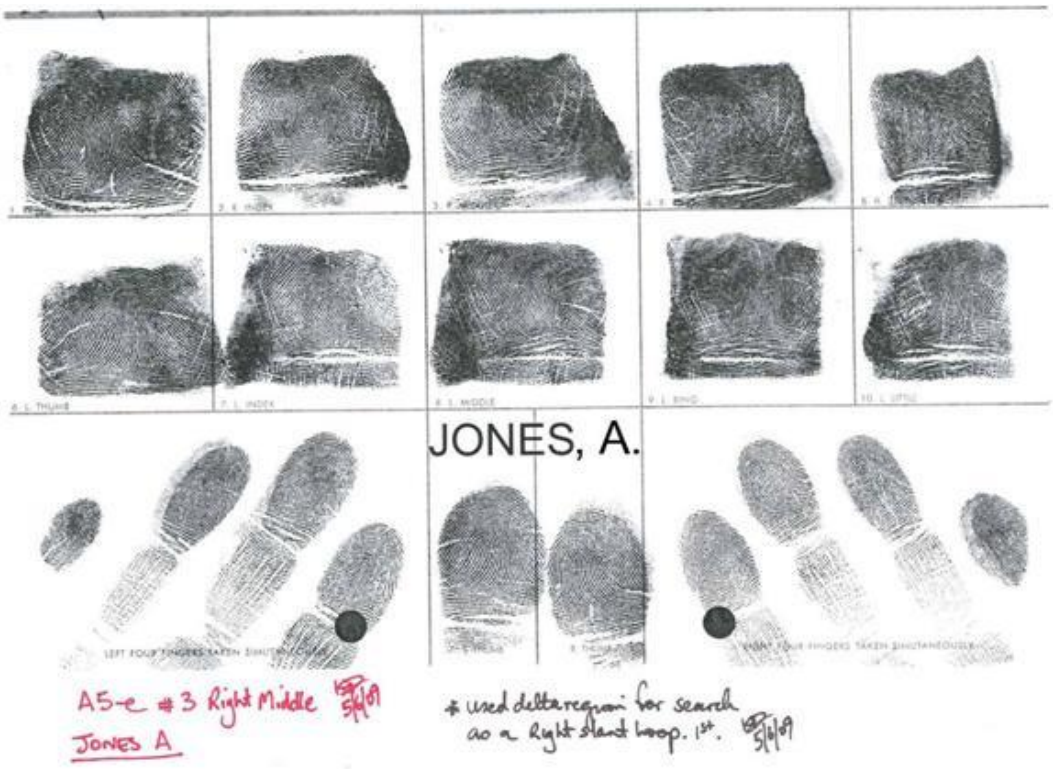

Figure 21 Example of a typical paper-and-ink ten print card. Source www.cplex.com.

Latent fingerprints. In AFIS, especially in those applied in forensic applications and law-enforcement, latent fingerprints are of great interest. These are fingerprint impressions (usually partial) left behind by an individual (usually a criminal) on a surface (in most cases at a crime scene). Such impressions are later recovered and digitized by forensic experts. The main difference with respect to the previous type of fingerprint data is that, in this case, the individual is not present at the time of the acquisition. Therefore, in the case of bad quality fingerprints (e.g. a very limited portion is only available) a re-acquisition is not possible.

Latent fingerprints are in general not clearly visible and their detection often requires some means of chemical development and enhancement. Powder dusting, ninhydrin spraying, iodine fuming, and silver nitrate soaking are the four most commonly used techniques of latent print development. Some typical examples of latent fingerprint are shown in Figure 22, where it can be observed that the quality is much lower than that of the inked and live-scanned fingerprints shown in Figures 19, 20 and 21.

Latent fingerprints are also referred to in the literature as fingermarks. While probably this is the most precise term (or simply marks), the most extended one is latent fingerprints (or simply latents). In the present report we will use this last term (latent fingerprints) to refer to this type of fingerprint data.

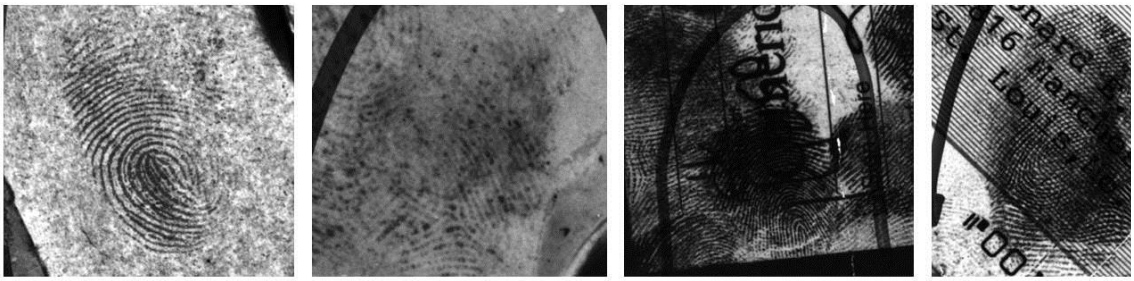

Figure 22 Typical examples of latent fingerprints. Source http://biometrics.cse.msu.edu/.

The reader should notice that this variety of fingerprint data (inked, live-scanned, flat, rolled, latents) poses a big challenge to AFIS that have to cope with all the possible types of fingerprint and match them against each other while maintaining high accuracy.

Annex 2: Comparative table between Prüm and SIS-II

Aspect	Prüm	Envisaged SIS-II with AFIS
Availability	24/7 but only maximum response time of 24 hours is guaranteed. Could be faster at certain times.	24/7 without restriction. Response time may only be limited by the available resources of the central database.
Accessibility	In the course of individual investigation cases.	"Administrative" purposes are excluded. Access take place in the course of controls at Schengen external borders and for checks conducted by Police and Customs authorities
Real-time Access	Not possible because of 24 hours constraint.	It is the case today for alphanumerical data and it is also expected for fingerprints
Accuracy	Individual response depends on the national AFIS and its configuration. No uniform thresholds whatsoever.	Would depend on thresholds agreed at central level.
Data size	Joint AFIS data of all connected countries, presumably in the range of tens of millions of persons.	Alerts related to persons (790 000) with fingerprints (97.000), presumably one million after deployment.
Degree of automation	Queries can be generated quite conveniently but response in each queried country needs to be triggered manually.	Interface and response should be comparable to state-of-the-art AFIS.
Level of received information	Only hit lists and reference data (dactyloscopic data and a reference number) in a first step. Additional information about certain hits needs to be requested via channels not specified in the Council Decision and with no time frame specification.	All information attached by the MS which has issued the alert in SIS-II, including full access to the relevant fingerprint data. Supplementary information can be requested from national SIRENE offices. According to SERENE manual section 1.13, the SIRENE Bureau shall answer all requests for information on alerts and hit procedures, made by the other Member States via their SIRENE Bureaux, as soon as possible. In any event a response shall be given within 12 hours. (See also Section 1.13.1. on indication of urgency in SIRENE forms).

This page is intentionally left blank.

Annex 3: Introductory note sent to MS prior the JRC visit

JRC study on AFIS technology for its introduction in the SIS-II database

Outline of Technical meeting with national AFIS Experts

USE CASES

What are the typical use cases for Member States with respect to their national AFIS and to future access to fingerprints in SIS?

For each use case:

- General description
- Specific examples
- Expected response time
- Type of response: single answer or ranked list
- Acceptable performance with respect to accuracy
- Type of data involved

AFIS SYSTEM

What national AFIS is in use?

What type of templates are involved?

Is it compatible with ISO/NIST standards or other standards?

Does it have a quality check and, if yes, when and how is it applied?

Is there a minimum quality threshold?

How are bad quality samples dealt with?

What performance/accuracy evaluation is available and how was it done?

What search filters does the AFIS have? For instance:

- Date of data
- Type of data (flat, rolled, latent…)
- Origin of data (country)
- Fingerprint class (right loop, left loop, whorl…)
- Quality of data

What is the level of human intervention?

When do expert examiners intervene in the process? What is their role?

How are the AFIS results checked?

Do you consider a totally lights-out scenario?

What type of maintenance of the AFIS system do you perform?

DATA

Do Member States have a centralized database or are the data otherwise organized?

Size and nature of the fingerprint data:

- Flat/Rolled?
- Inked/live-scanned?
- Latent?

Do you consider composite ten print cards?

Do you keep a database of fingerprints? Is it a separate database to that of ten prints?

How are the ten print cards acquired?

What methodologies do you use for the development of latent fingerprints?

What experience exists on interoperability of data obtained by different methodologies?

Do you have any statistics on the quality of the different types of fingerprint data?

Is there a minimum number of minutiae for a fingerprint to be stored?

Is data flagged according to its type/quality/origin…?

How is the upload process of fingerprints into SIS-II organized?

What methodologies do you apply to ensure the integrity of the enrolled data?

LIVE DEMO

Possibility of real operational demo on the AFIS in use?

Possibility of quality checks on the database or parts of it?

LB-NA-27473-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/50621

ISBN 978-92-79-51929-1